DS-Mobile Client Installation & User Guide (MODERN-UI)

© Asigra Inc. All Rights Reserved.
Confidential.

Assumptions

The following assumptions are made about the audience for this document:

Familiarity: User is familiar with the Operating System platform. User is familiar with basic Internet browsing.

Correct Input: User enters the correct data (e.g. user names, passwords, etc.) when asked or required. If invalid data is entered, an error message will appear, and you will be forced to correct the error before you may proceed.

Canceling activities: The option to cancel the current activity (in some cases the option is “No”) will exit the activity.

Disclaimer

Information in this document is subject to change without notice and does not represent a commitment on the part of ASIGRA Inc.

ASIGRA Inc. makes no representation or warranty, express, implied, or statutory, with respect to, and assumes no responsibility for the accuracy, completeness, sufficiency or usefulness of the information contained herein.

This document may contain sample screen shots, used to demonstrate Asigra Cloud Backup™ procedures. All information appearing in this document is used for illustration purposes only, and it should be considered fictitious.

Copyright

The software described in this document is furnished under a license agreement. It is against the law to copy the software on any medium except as specifically allowed in the license agreement.

Asigra, the Asigra logo, DS-Client, DS-System, and Cloud Backup are trademarks of Asigra Inc. All other brand and product names are, or may be trademarks of their respective owners.

About Asigra Cloud Backup™

Asigra Cloud Backup™ is a unique alternative to traditional backup methods, replacing conventional tape based systems with a fully automated Online solution. It provides centralized and automated backups of PCs, file servers and application/database servers with secure offsite storage and immediate Online restoration.

The system uses a DS-Client, installed onto the customer network, which hosts the Asigra Cloud Backup™ client application software that performs the backup and restore activity.

Document Prepared by:	
Asigra Inc.	
1120 Finch Avenue West, Suite 400	
Toronto, Ontario, CANADA M3J 3H7	
info@asigra.com	
www.asigra.com	

© Asigra Inc. All Rights Reserved. Confidential.

Document Revision History Table

This shows the major changes made to this document from version to version.

Version/Date	Notes
v12.2 [Revision Date: June 13, 2013]	
	• “Installation Guide” on page 6 • “User Guide” on page 15

© Asigra Inc. All Rights Reserved.
Confidential.

Installation Guide 6

Before you install or upgrade 7
I) Supported Platforms 7
II) Hardware & Software Minimum Requirements 8
III) Obtain the DS-Mobile Client Installation Program 8
IV) Select your encryption key(s) 8
V) Log in to target installation computer 9

Run the DS-Mobile Client Installation Program 10
Step 1. Run Installation Package 10
Step 2. Select Installation Location 10
Step 3. Specify the DS-Mobile Client Service Logon Account 10
Step 4. Complete the Wizard 11
Step 5. Connect to DS-Mobile Client and perform initial configuration 11
Custom 'Wrapped' Installation 13

After Running the Installation 14
Connect to DS-Mobile Client and perform initial configuration 14

User Guide 15

Login 16
Asigra UI window 17

Working with Backup Sets 19
New Backup Sets 19
Backup (Scheduled & On-Demand) 24
Restore 26
Delete 30
Synchronize 31
Change Credentials 31
Edit a Backup Set 32

Configuration & Logs 33
Admin 33
Re-Register 34
Recovery 35
DS-Mobile Client Configuration Tool 36
Logs 39
To update a DS-Mobile Client using 'config-update.xml' 40
About 41
SAMPLE 'config-update.xml' file 42
Customizing the 'config-update.xml' file 45
SAMPLE 2: 'config-update.xml' file to assign DS-Mobile Client Roles 46
SAMPLE 2: Customizing the 'config-update.xml' file to assign DS-Mobile Client Roles 46

Knowledge Base 47

Backup & Restore of individual E-Mails from Microsoft Outlook 48

Troubleshooting: Remote backup of Windows 7 / Windows 8 files requires a Microsoft patch and some configurations 51

Centrally Managed Backup Policy 52

© Asigra Inc. All Rights Reserved.
Confidential.

DS-NOC monitoring connections 54

Dialog Help 56

© Asigra Inc. All Rights Reserved.
Confidential.

Installation Guide

This section contains the installation instructions.

© Asigra Inc. All Rights Reserved.
Confidential.

Before you install or upgrade

I) Supported Platforms

Platform	Version	MSI-Deployment Compatible *
Windows® XP x86 (32-bit)	• Professional SP3 • Home SP3	• **Yes** • NO
Windows® XP x64 (64-bit)	• Professional SP2	• **Yes**
Windows® 2003 Server** x86 (32-bit)	• Standard SP2 • Standard R2 SP2 • Enterprise SP2 • Enterprise R2 SP2	• NO
Windows® 2003 Server** x64 (64-bit)	• Standard SP2 • Standard R2 SP2 • Enterprise SP2 • Enterprise R2 SP2 • Data Center SP2	• NO
Windows® VISTA x86 (32-bit) or x64 (64-bit)	• Ultimate SP2 • Enterprise SP2 • Home Basic SP2 • Business SP2 • Home Premium SP2	• **Yes** • **Yes** • NO • **Yes** • NO
Windows® 2008 Server** x86 (32-bit)	• Standard SP2 • Standard R2 SP1 • Enterprise SP2 • Enterprise R2 SP1	• NO
Windows® 2008 Server** x64 (64-bit)	• Standard SP2 • Standard R2 SP1 • Enterprise SP2 • Enterprise R2 SP1 • Data Center SP2 • Data Center R2 SP1	• NO
Windows® 7 x86 (32-bit)	• Starter SP1 • Home Basic SP1 • Home Premium SP1 • Ultimate SP1 • Enterprise SP1 • Professional SP1	• NO • NO • NO • **Yes** • **Yes** • **Yes**
Windows® 7 x64 (64-bit)	• Home Premium SP1 • Ultimate SP1 • Enterprise SP1 • Professional SP1	• NO • **Yes** • **Yes** • **Yes**
Windows® 8 x86 (32-bit) or x64 (64-bit)	• Windows 8 • Pro • Enterprise	• NO • **Yes** • **Yes**
Windows® 2012 Server** x64 (64-bit)	• Essentials • Standard • Datacenter	• NO • NO • NO

** Refers to DS-Mobile Client MSI Deployment via Active Directory capability (for instructions, see "DS-Mobile-Client-Mass_Deployment_User_Guide.pdf").*

*** You can install DS-Mobile Client on Windows 2003/2008/2012 Server. However, you cannot create backups of the local machine (Windows Server Operating System backup sets are not supported).*

© Asigra Inc. All Rights Reserved. Confidential.

Note: DS-Mobile Client does not support backup / restore of Windows **Server** Operating Systems. You will not be able to create a backup set if the target computer is running any Windows Server OS.

II) Hardware & Software Minimum Requirements

You should use the best hardware possible to maximize Asigra Cloud Backup™ performance. If applicable, it is strongly recommended that you use the fastest brand-name components available.

Hardware	x86 (32-bit) or x64 (64-bit) Architecture
CPU (1 or 2)	2 GHz or greater
RAM	1 GB RAM if > 1 Million Files, or 2 GB RAM if multiple files > 1 GB
Free disk space for app. and buffer	1 GB or more

Note: To run this application, the Microsoft .NET Framework (v 4.0.30139) must be installed.

III) Obtain the DS-Mobile Client Installation Program

Contact your Asigra Cloud Backup™ Service Provider to register. You will be provided with:

- Installation Disc (or download from Service Provider Website);
- Your Customer Account number: _____;
- Your DS-Mobile Client number: _____;
- The DS-System IP address: _____;

Write these numbers down (a space is provided for each above). They are required after you finish the installation when you first launch the User Interface (see: "Step 5. Connect to DS-Mobile Client and perform initial configuration" on page 11).

- Alternatively, your service provider may provide a download of a Custom 'Wrapped' Installation with all these selections pre-loaded (see: "Custom 'Wrapped' Installation" on page 13).

IV) Select your encryption key(s)

- Data backed up through the DS-Mobile Client is encrypted using the encryption key(s) you specify.
- Encryption keys are set once. You cannot change the key(s) once set. The DS-Mobile Client service will not be allowed to start.
- You must select the type of encryption key (DES, AES 128-bit, AES 192-bit, AES 256-bit). Stronger encryption requires longer keys (8, 16, 24, or 32 characters).
- **Private key**: You must set this key.
- **Account key**: If you only have one DS-Mobile Client, you do not need to set this key. When you have more than one DS-Mobile Client (or regular DS-Client), you must specify an Account key. This must be the same for every DS-Mobile Client / DS-Client that is registered under this same customer account on the DS-System. Common data from your DS-Mobile Client(s) / regular DS-Clients will be encrypted using the Account key.

© Asigra Inc. All Rights Reserved. Confidential.

V) Log in to target installation computer

- Make sure you have logged on as the target DS-Mobile Client computer's Administrator (or a user with equivalent privileges).

© Asigra Inc. All Rights Reserved.
Confidential.

Run the DS-Mobile Client Installation Program

Step 1. Run Installation Package

Depending on your selections, some different screens will appear. These differences are noted below.

1. [**Option A**] Run the installation program from the download directory or from the corresponding folder on the installation DVD:

   `\Software\DS-Client\DS-Mobile_Client\install.exe`

   [**Option B**] Run the Asigra Cloud Backup™ Installation Center for Windows Products (**setup.exe**) located in the root directory of the installation DVD.
   - The Installation Center is a common launcher for all Windows-platform installations. It allows you to choose the specific installation package you want, without the need to browse the installation DVD.

   [**Option C**] Run a custom 'wrapped' installation supplied by your Service Provider (usually downloaded from their Web Site).
   - For this type of installation, skip to "Custom 'Wrapped' Installation" on page 13.
2. Choose the Setup Language:
   - English
   - German

   Note: The selected language will be installed for the DS-Mobile Client service. Once set, the DS-Mobile Client Service language cannot be changed (for logs and popup messages).
3. Follow the GUI to install DS-Mobile Client. A "Verify Prerequisites" screen appears.
   - Click "Next".
4. The License Agreement page appears. You must accept the license agreement to continue. Click Next.

Step 2. Select Installation Location

1. Specify the target folder.
   - The default is: **C:\Program Files\CloudBackup\DS-Mobile Client**
2. Click Next.

Step 3. Specify the DS-Mobile Client Service Logon Account

1. The "Specify the DS-Mobile Client Service Logon Account" screen appears allowing you to choose the user account and password on the DS-Mobile Client computer that will be used by the service.
   - You can skip this page by leaving the fields empty and clicking "Next", which means the "LocalSystem" account will be used for the service.
   - If you specify a user, it must be a member of the local computer's "Administrators" group.
     - If you specify the same user account and password as you are currently logged into the Windows computer with, the Asigra UI will use those credentials to automatically log into the DS-Mobile Client when it is launched.
2. Click Next.

© Asigra Inc. All Rights Reserved.
Confidential.

Step 4. Complete the Wizard

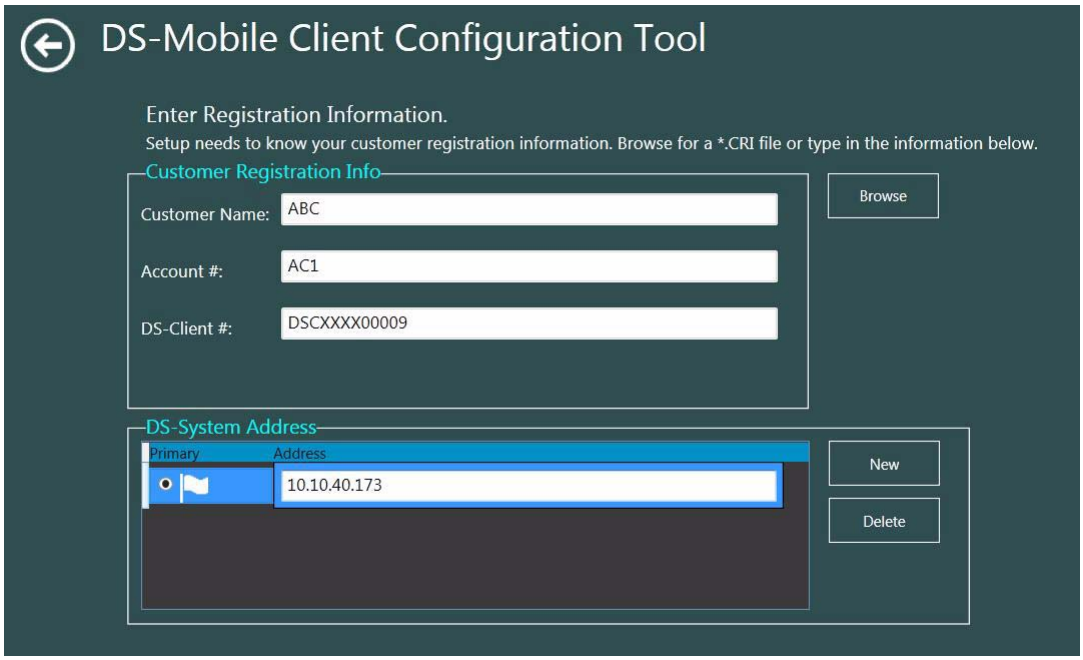
1. The “Completing the Wizard” screen appears once all files are copied.
2. Click “Finish“ to complete the installation.
   - By default, “Run DS-Mobile Client and User Interface now” is selected, which will start the DS-Mobile Client service and launch the GUI.

Note: If you are using an older version than Windows 8, the operating system may be missing the required “Microsoft .Net framework 4.0” that is required to run the “Modern-UI” version. If this component is missing, you will be prompted to download and install it.

Step 5. Connect to DS-Mobile Client and perform initial configuration

On connection to a DS-Mobile Client that has not registered with the DS-System, you will encounter a “DS-Mobile Client Configuration Tool” wizard where you must enter this information.

1. Launch the GUI.
   - If the “Login” screen appears, you must enter your Credentials.
2. After you successfully connect to the DS-Mobile Client, the “Enter Registration Information” screen appears.



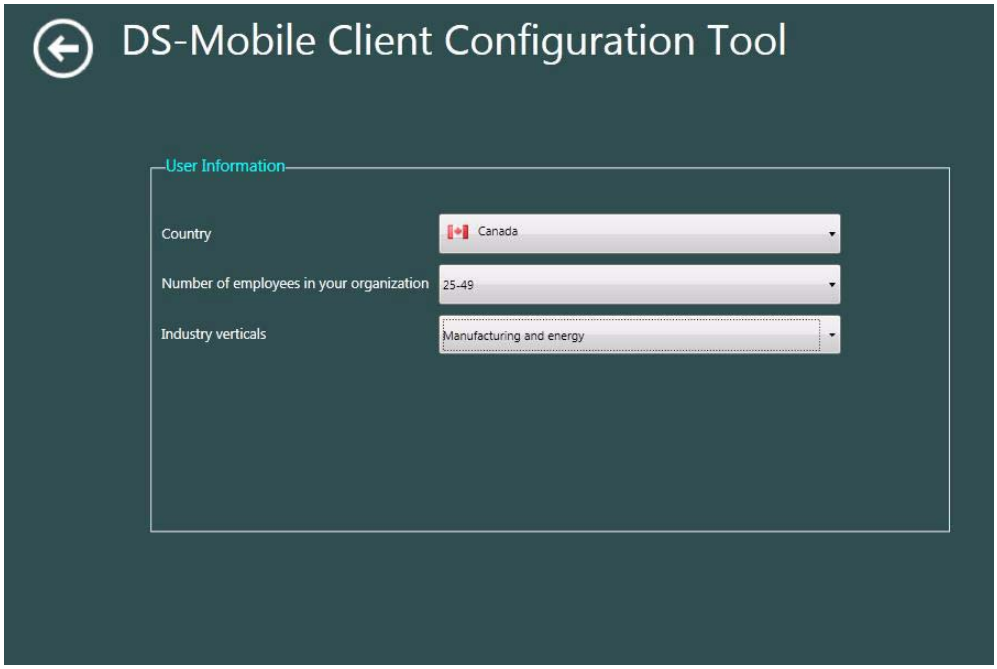
3. Enter the appropriate information in each field of the screen.

Name	Enter a descriptive name for this DS-Mobile Client.
Account #	Enter your Account number.
DS-Client #	Enter your DS-Mobile Client number.
Browse	An alternative to manually entering the above information is to use a .CRI file supplied by your Service Provider. Click Browse to search for this file.

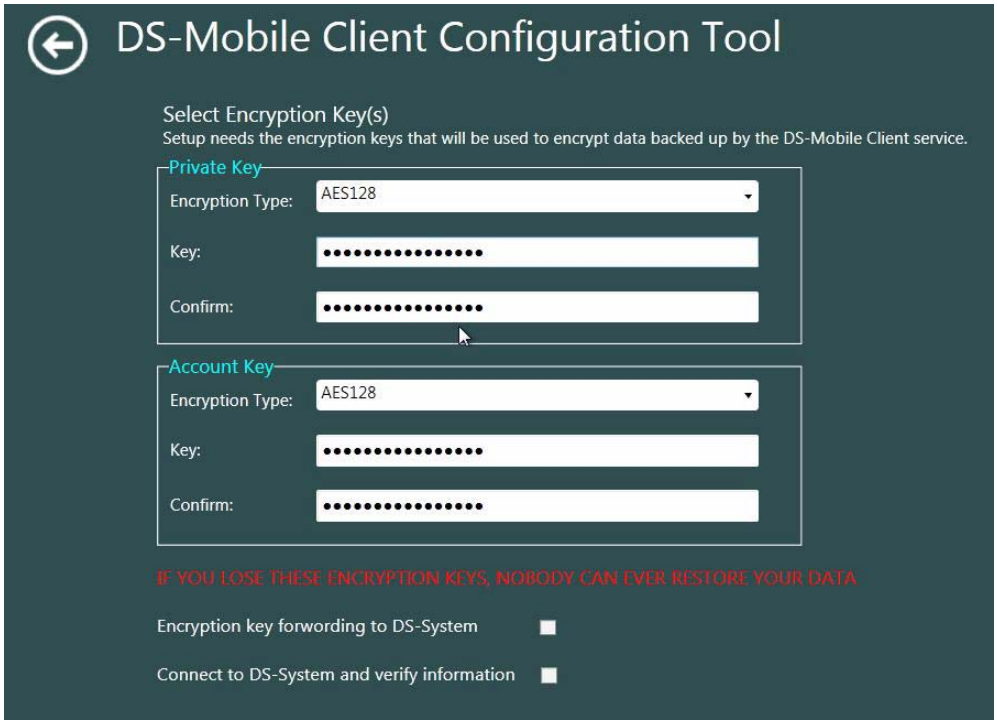
4. Your Account and DS-Client numbers must match those provided to you by your Service Provider System (see: III) Obtain the DS-Mobile Client Installation Program in the Before You Install section).

© Asigra Inc. All Rights Reserved.
Confidential.

5. Enter the IP address of the DS-System your DS-Client will be using. Your Service Provider may have more than one IP address for the DS-System, if this is the case you can specify any or all of them. The same applies for N+1 DS-Systems.
   - Use a semi-colon (;) to separate each IP address.
6. Click “Next”. The “DS-Mobile Client Configuration Tool” switches to its “User Information” screen.



   - You must supply the requested information about your organization by choosing from the drop-down list options.
7. Click “Next”. The “DS-Mobile Client Configuration Tool” switches to its “Select Encryption Key(s)” screen.



© Asigra Inc. All Rights Reserved.
Confidential.

8. In this screen, you must set the encryption key that the DS-Mobile Client will use. (See: IV) Select your encryption key(s))
   - Choose an encryption type (DES or AES) and level (# of bits) from the list.
   - An encryption key is case sensitive. Its length (in characters) depends on the type and level of encryption selected. DES requires 8 characters, AES-128 requires 16 characters, AES-192 requires 24 characters, and AES-256 requires 32 characters. For better security, do not use dictionary words or proper names, and try to randomly mix numbers in with the letters.
   - Auto-complete feature: If you do not specify the full amount of characters in the Key field, installation will fill in the remainder by repeating the string of characters you have entered. (e.g. entering “123” with AES-128 will generate an encryption key of “1231231231231231”, or entering “a” for DES will generate the encryption key “aaaaaaaa”).
   - Keep the key(s) in a secure location. It is necessary if you ever need to reinstall your DS-Client (e.g. if the computer was destroyed in a disaster) to a new computer.
9. **Private Key**: You must set the private key for your DS-Mobile Client.
   - Backup data from your DS-Mobile Client installation will be encrypted with this key.
10. **Account Key**:
    - Common backup data from all your DS-Mobile Client / regular DS-Client installations will be encrypted with this key.
11. **Encryption key forwarding to DS-System**:
    - Check to have DS-Mobile Client forward the encryption key(s) to the DS-System the first time it connects with DS-System.

      NOTE: If you forward the keys, they will remain encrypted on the DS-System. However, your Service Provider will be able to create a valid .CRI file containing the encrypted keys. This file will be able to recreate a working version of this DS-Mobile Client. Make sure this conforms to your security policies before enabling this option.
12. Once you have made all the initial DS-Mobile Client configurations, click “Finish” to register with the DS-System.
    - If registration is successful, you will be able to use DS-Mobile Client immediately. Refer to the DS-Mobile Client User Guide for more information.

Custom ‘Wrapped’ Installation

If you downloaded the installation from your Service Provider’s Web Site, it will probably be their customized version. This simplified, ‘custom wrapped’ installation already contains several pre-defined selections, therefore you will only need to select the language, agree to the license, choose a Private Encryption Key, and enter your E-Mail address:

1. Choose the Setup Language:
   - English
   - German
2. The License Agreement page appears. You must accept the license agreement to continue. Click Next.
3. Select a Private Encryption Key. You must choose the type (strength), and provide the key and confirm it a second time.
4. Enter your E-Mail address.
5. Click Next to complete the installation.
   - The Cloud Backup GUI will start if the installation completes successfully.

© Asigra Inc. All Rights Reserved. Confidential.

After Running the Installation

Connect to DS-Mobile Client and perform initial configuration

Once you launch the User Interface and connect to a DS-Mobile Client that has not registered with DS-System, you will encounter the DS-Mobile Client Configuration Tool wizard.

- See “DS-Mobile Client Configuration Tool” on page 36.

© Asigra Inc. All Rights Reserved.
Confidential.

User Guide

The DS-Mobile Client is targeted towards the mobile computing market (laptops). To keep the instructions simple, the user guide and installation instructions are included in the same document.

The DS-Mobile Client interface is the “Asigra UI”, which gives customers fast and reliable control over their backups.

Note: This guide has been written using screenshots from the “Modern-UI” version. There is also a “classic” version of the GUI that is also installed in the same folder. There are some differences in the look and feel, but the general features described are the same.

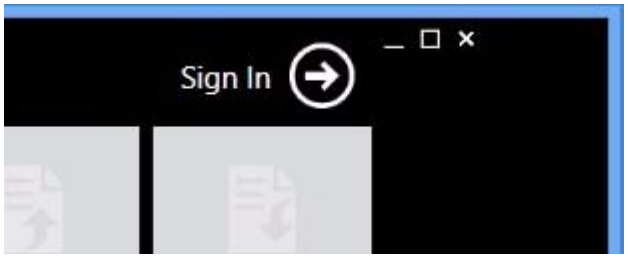
© Asigra Inc. All Rights Reserved.
Confidential.

Login

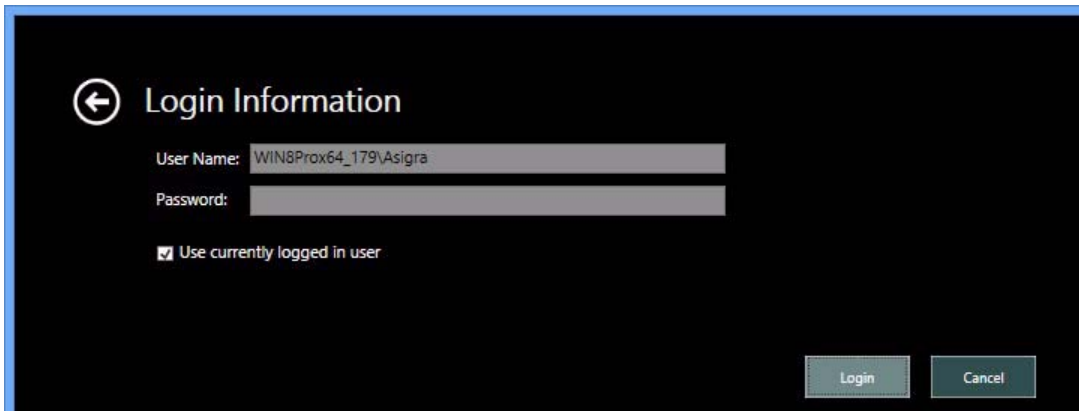
Note: By default, this login step is skipped and your current logged in user will be used to login to DS-Mobile Client. If that login fails (or if you logout), you can follow these steps to supply another user account for login.

You can only login to the DS-Mobile Client computer with a user account that is a member of the local computer's Administrators group or from the Domain Administrators group.

1. Start > Programs > Asigra DS-Mobile Client > Asigra UI (On Windows 8, you can just type "DS-Mobile" in the "Start" window.) The User Interface window appears.
2. Click the "Sign In" button.



3. The Login screen appears.



Dialog Help: See "Login" on page 60.

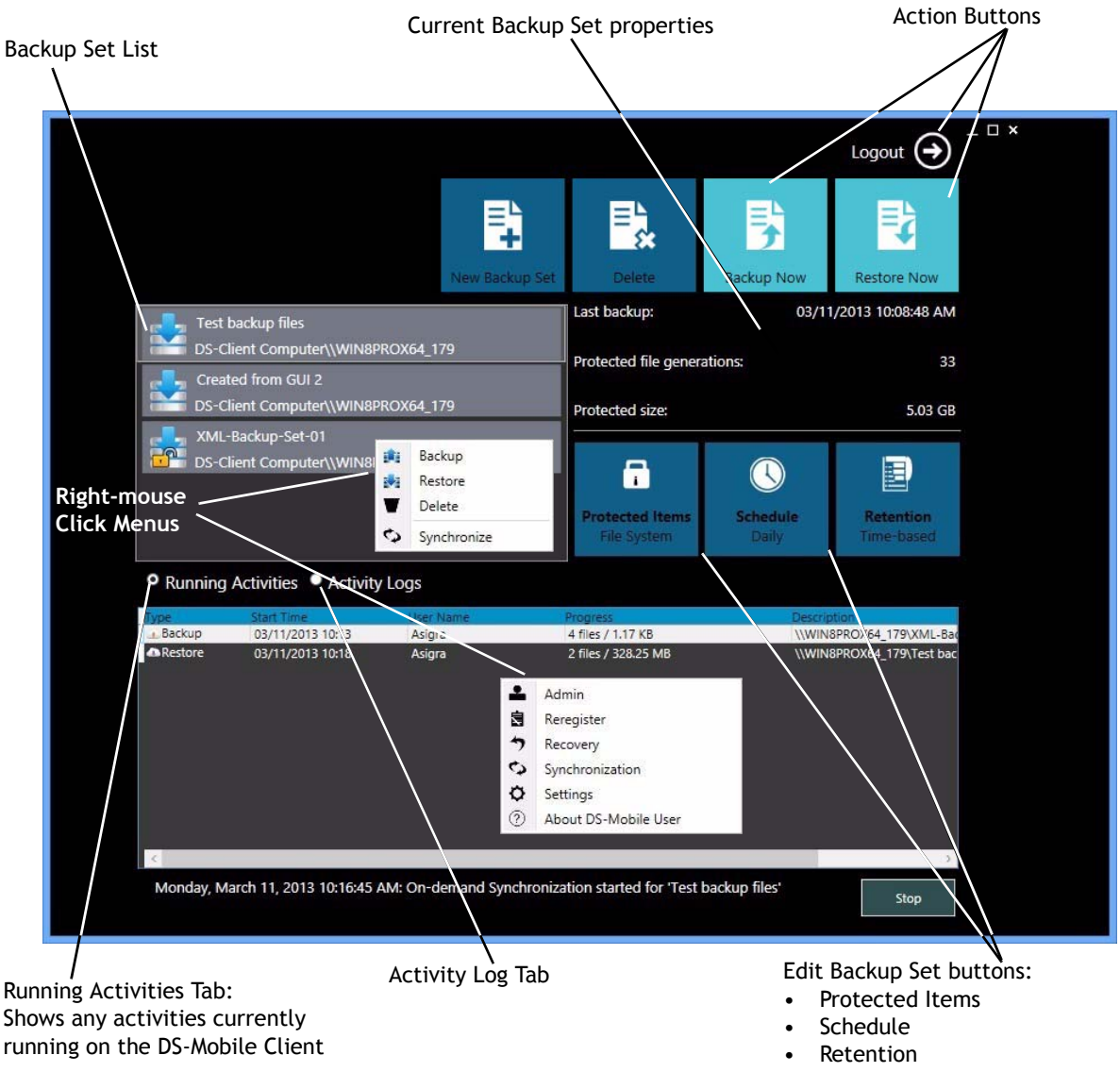
Note: The "From" option only appears if the DS-Mobile Client computer belongs to a Windows Domain.

4. Enter your Credentials and press "Login".
   - Select "Use currently logged in user" if you want to use your current Windows login and password to automatically connect to DS-Mobile Client when you launch the Asigra UI.
5. If successful, the Asigra UI window activates.
   - See "Asigra UI window" on page 17.

© Asigra Inc. All Rights Reserved.
Confidential.

Asigra UI window

To access functions, you can select from the menu options found directly below the title bar, in the Asigra UI window:



Dialog Help: See "Main Window" on page 59.

Title Bar	Shows the login name and location (usually 127.0.0.1 for the local computer / laptop).
Backup Set List	Shows a list of the backup sets that have been defined on the DS-Mobile Client. If you click on a backup set, its properties are displayed to the right. The Action and Edit buttons will activate or be grayed out, depending on what can be performed. • You can highlight a backup set with the mouse or use the arrow keys to cycle through each set in the list. • To rename a backup set, double-click on its name.

© Asigra Inc. All Rights Reserved.
Confidential.

Action Buttons	The action buttons (except New Backup Set) work on the backup set highlighted in the Backup Set List. • New Backup Set: See “New Backup Sets” on page 19. • Delete: See “Delete” on page 30. • Backup Now: See “Backup on demand” on page 24. • Restore Now: See “Restore” on page 26.
Edit Buttons	The Edit buttons work on the backup set highlighted in the Backup Set List. See “Edit a Backup Set” on page 32. • Protected Items • Schedule • Retention
Running Activities Tab	Shows any activities that are currently running on the DS-Mobile Client. If possible, you can use the Stop button to end the highlighted activity.
Activity Log Tab	Shows a list of all the activities logged by the DS-Mobile Client. You can filter the list by date. • See “Logs” on page 39.

© Asigra Inc. All Rights Reserved.
Confidential.

Working with Backup Sets

Activities on DS-Mobile Client center around individual backup sets. Once you have created a backup set, you can perform all the other related activities to it.

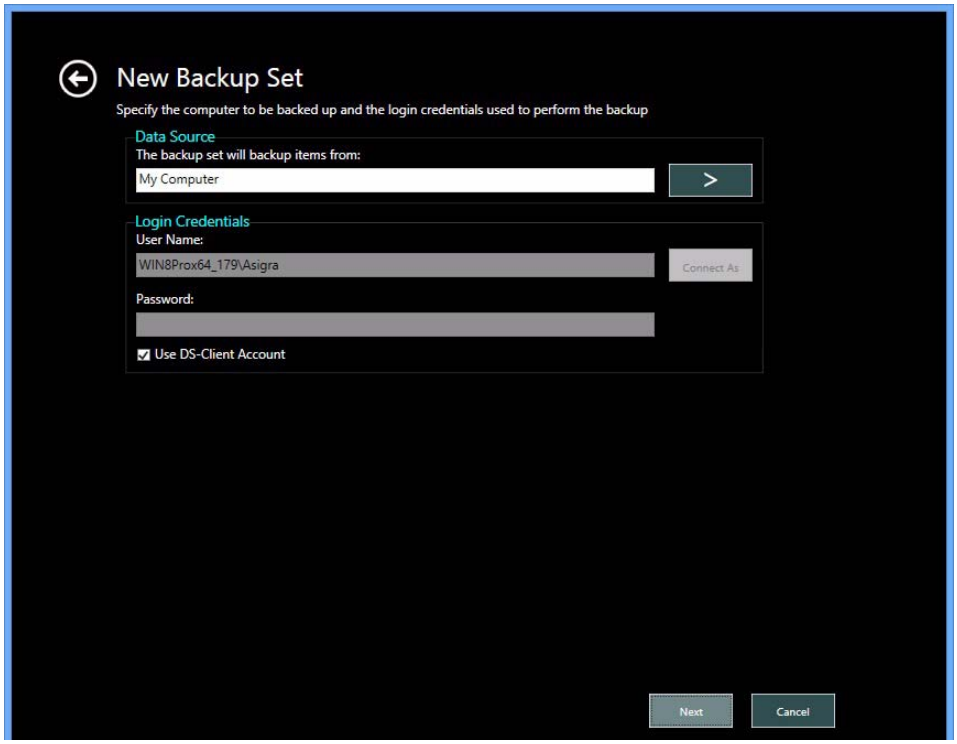
- "New Backup Sets" on page 19
- "Backup (Scheduled & On-Demand)" on page 24
- "Restore" on page 26
- "Delete" on page 30
- "Synchronize" on page 31
- "Change Credentials" on page 31

New Backup Sets

You must create at least one backup set.

1. Click "New Backup Set".

2. The New Backup Set Wizard appears on the "Data Source and Login Information" tab.



Dialog Help: See "Data Source and Login Information" on page 57.

- Select the Data Source. Normally, for laptops, you would use the default "My Computer" selection. If connected to the cloud (network), you can browse to select another machine.
- In the "Login Credentials" section, select the user account that DS-Mobile Client will use to access the files on the data source. The default is the same user name as the one currently used to log in through the Asigra UI.

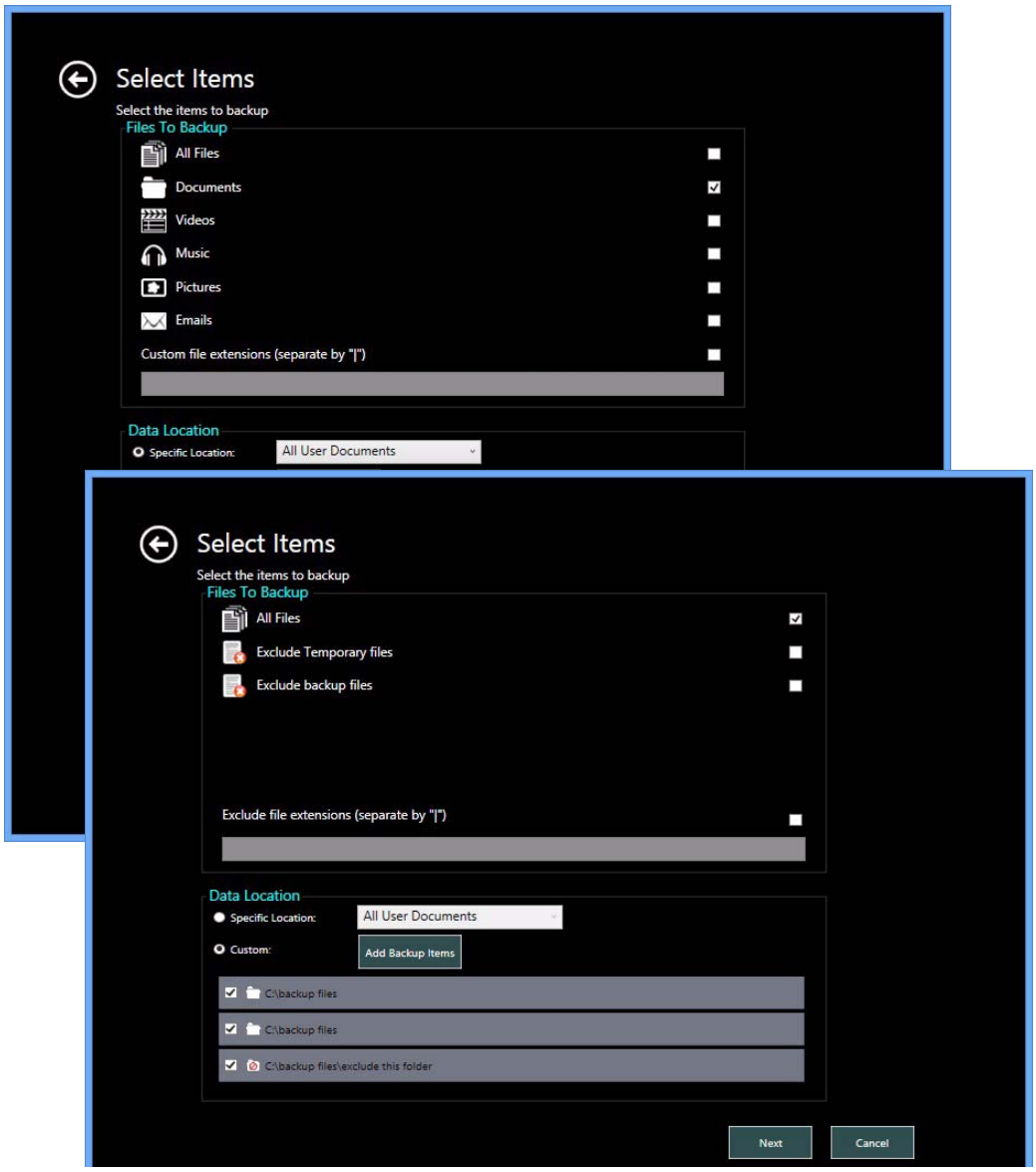
© Asigra Inc. All Rights Reserved.
Confidential.

- If you have selected another computer, you must supply valid access credentials to the selected machine.
- Specify the user name in the following format:

```
<computer-name_or_domain-name>\user-name
```

Where: <computer-name_or_domain-name> is either the computer name or domain name where the corresponding user-name is defined.

3. Click Next to continue. The New Backup Set Wizard appears on the “Select items” tab.

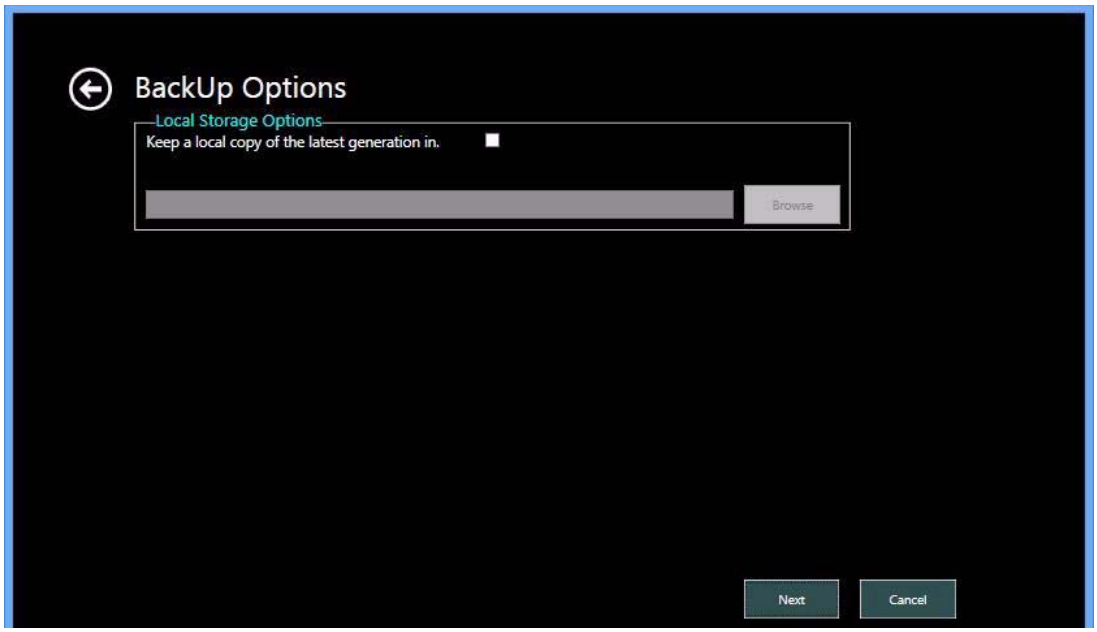


Dialog Help: See “Select Items (New / Edit Backup Set)” on page 62.

- In the “Files To Backup” section, select the type(s) of files to backup. This will apply a filter to the backup location(s) selected.
- In the “Data Location” section, select the folder(s) to backup or exclude. You can click “Add Backup Items” to open a popup wizard browser to select the target data location(s).

© Asigra Inc. All Rights Reserved.
Confidential.

4. Click Next to continue. The New Backup Set Wizard appears on the “Backup Options” tab.



Dialog Help: See “Backup Options” on page 56.

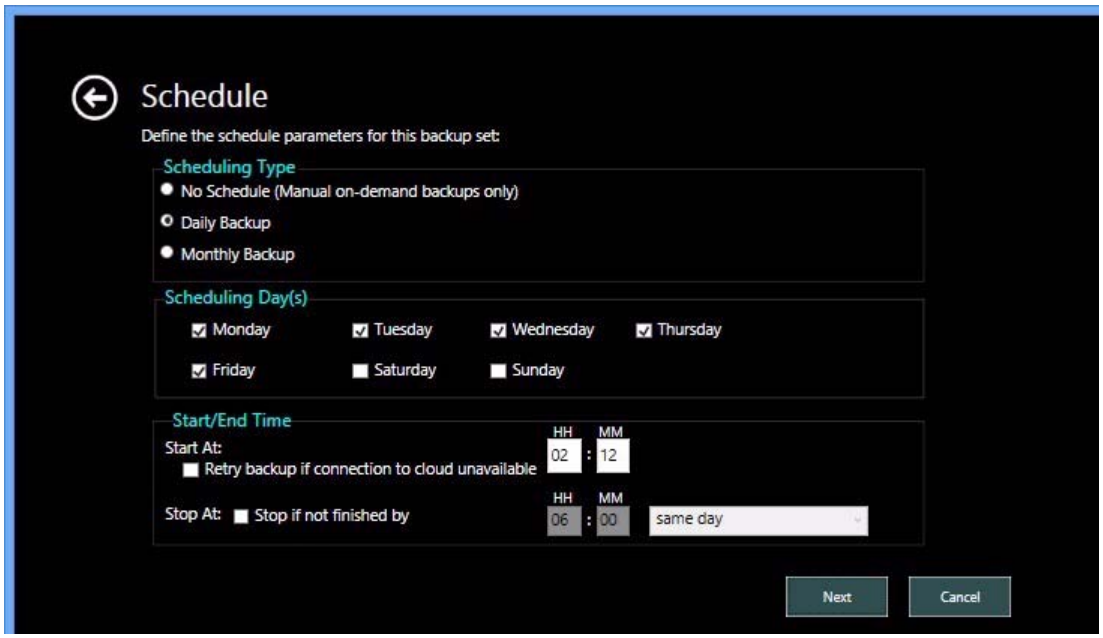
- This screen’s setting is optional (you do not have to make a selection).
- “Keep a local copy of the latest generation in”: If you select this option, it means a copy of the latest generation of all selected backup items will be saved to this folder on the local machine. Click “Browse” to select the folder to use.
- Make sure you have enough space in that location to accommodate the backup
- The advantage of a local copy is that restores will be faster, but the cost is additional space on your local computer.

NOTE: This option only appears if the Tool has been enabled by your Service Provider from the DS-System side.

NOTE 2: This local storage location is also a local storage ‘cache’ location. If the connection with the DS-System fails during backup, DS-Mobile Client will save backup data to this local storage cache. Once the connection to DS-System is re-established, DS-Mobile Client will send the data from the local storage cache.

© Asigra Inc. All Rights Reserved.
Confidential.

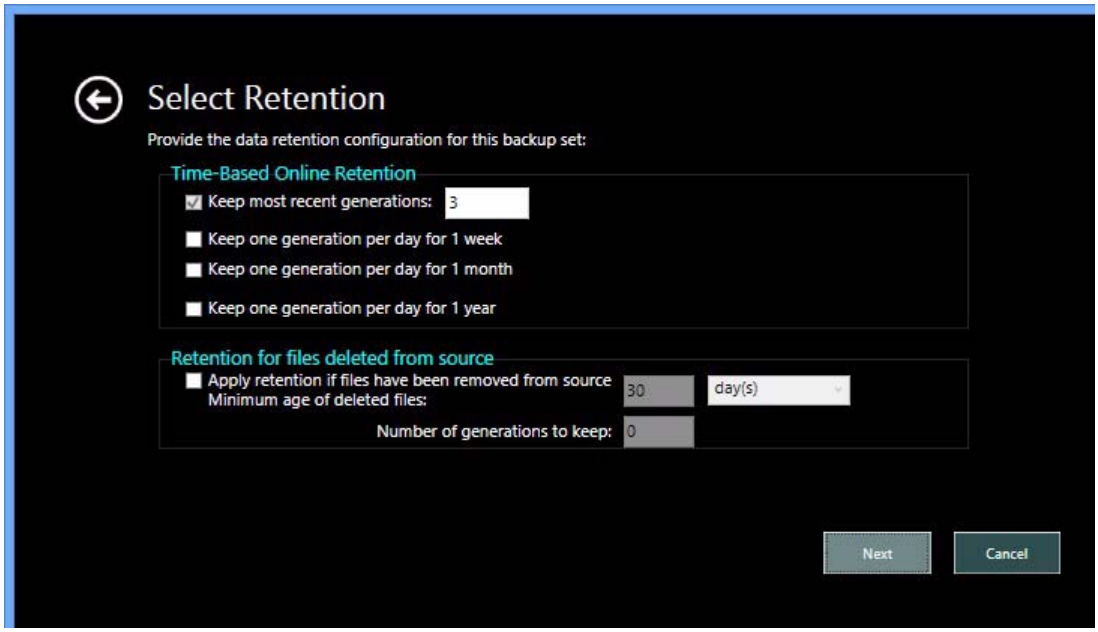
5. Click Next to continue. The New Backup Set Wizard appears on the “Select Schedule” tab.



Dialog Help: See “Select Schedule” on page 65.

- In the “Scheduling Type” section, select the frequency of the scheduled backups.
- In the “Scheduling Day(s)” section, what day(s) this backup will be scheduled to run.
- In the “Start / End Time” section, select when the backup will start and any other time limitations.

6. Click Next to continue. The New Backup Set Wizard appears on the “Select Retention” tab.


Select Retention
Provide the data retention configuration for this backup set:
Time-Based Online Retention
Keep most recent generations:
3
Keep one generation per day for 1 week
Keep one generation per day for 1 month
Keep one generation per day for 1 year
Retention for files deleted from source
Apply retention if files have been removed from source
Minimum age of deleted files:
30
day(s)
Number of generations to keep:
0
Next
Cancel

Dialog Help: See “Select Retention” on page 64.

- In the “Time-based Online Retention” section, select how the backup set’s data will be retained online. Retention means “what data you want to keep

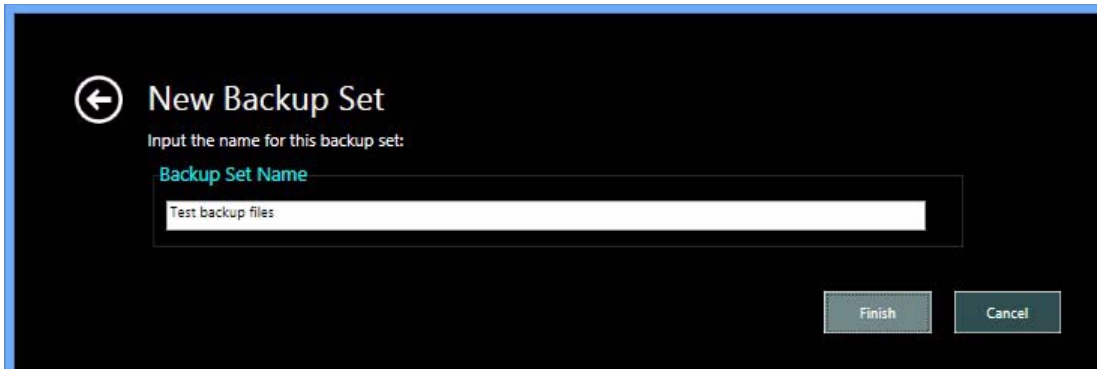
© Asigra Inc. All Rights Reserved.
Confidential.

online" and with DS-Mobile Client, you can select either by the number of generations or by the time data has remained online.

- The "Retention for files deleted from source" section is optional. These options only apply to files that the DS-Mobile Client detects have been removed from the backup source.

Note: On DS-Mobile Client, time-based retention automatically runs after every backup process.

7. Click Next to continue. The New Backup Set Wizard appears on the "Select Backup Set Name" tab.



Dialog Help: See "Select Backup Set Name" on page 61.

- Specify a name and press "Finish".
- The backup set will appear in the list on the main Asigra UI window.

Note: If you need to change the backup set name afterwards, you can double-click on it in the main Asigra UI window.

© Asigra Inc. All Rights Reserved.
Confidential.

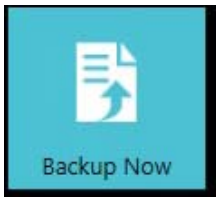
Backup (Scheduled & On-Demand)

When you create a backup set, you must specify a backup schedule (or choose the “No schedule” option). You can always backup on-demand.

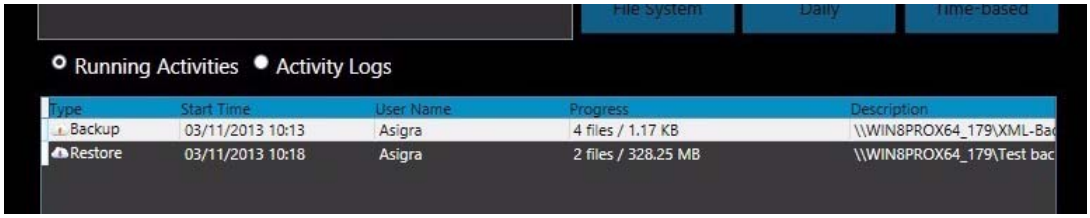
- See “Backup on demand” on page 24.
- See “Schedule a backup set” on page 25.

Backup on demand

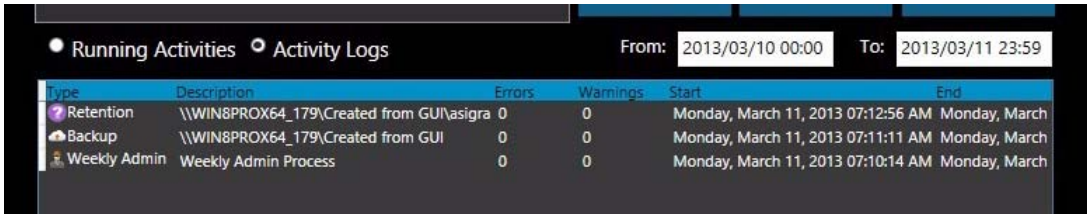
1. Highlight the backup set you want.
2. Click “Backup Now” or right-mouse click > Backup.



3. The backup will start immediately.



4. Check the Activity Log Tab for results.



5. If you see any errors, you can check the Event Log.
   - See “Logs” on page 39.

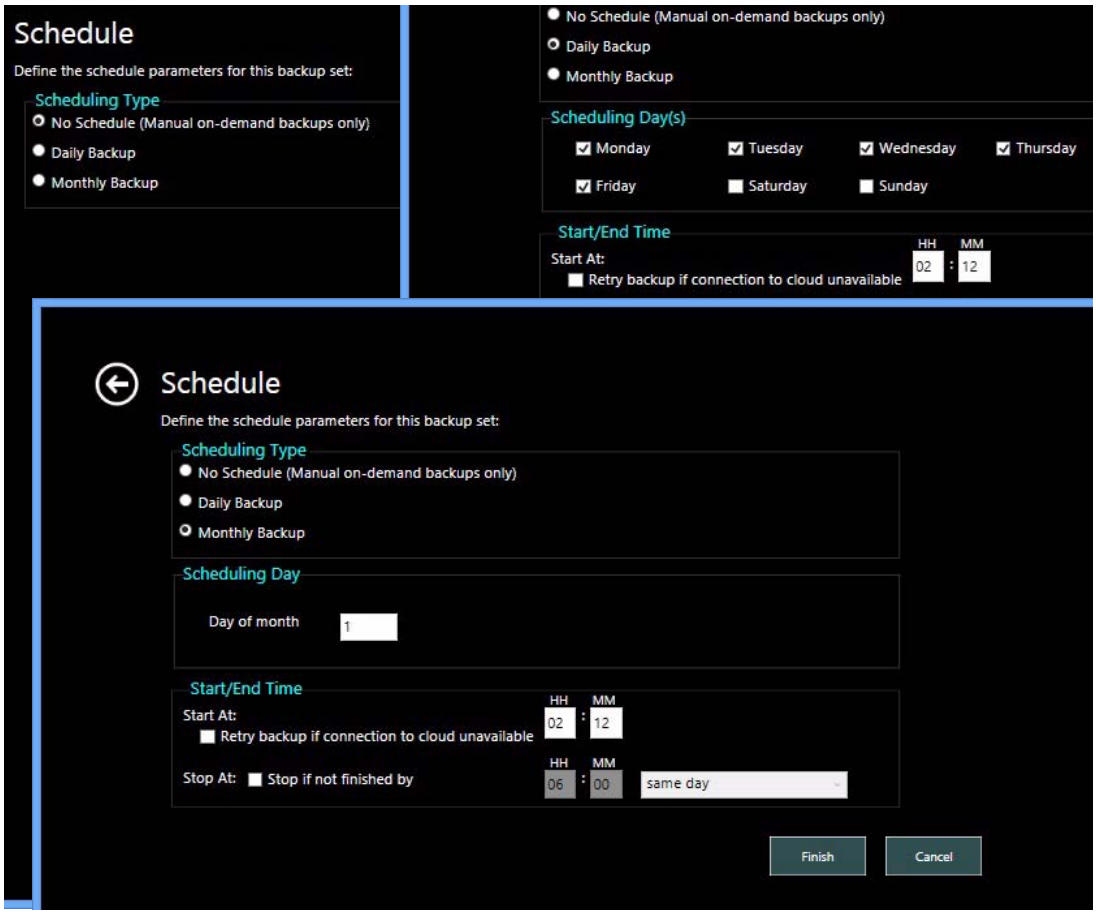
© Asigra Inc. All Rights Reserved.
Confidential.

Schedule a backup set

Schedules are designed for automatic, unattended backups. At any time, you can alter the schedule of a backup set, or select the “No schedule” option. For DS-Mobile Client schedules, the backup task always includes a retention task that follows the backup.

1. Highlight the backup set you want.
2. Press the “Schedule” button on the right-side of the Asigra UI.

3. The “Select Schedule” tab appears. The content changes, depending on the Schedule Type that is selected.



Dialog Help: See “Select Schedule” on page 65.

4. This is the same tab that appears when creating a new backup set.
5. Edit the schedule, as required, and click “Finish”.

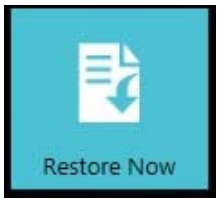
NOTE: If the laptop computer is powered off or the DS-Mobile Client service is not started, any schedules that were missed will attempt to be triggered if the machine or the service is started within six (6) hours from the time the schedule was supposed to run.

© Asigra Inc. All Rights Reserved.
Confidential.

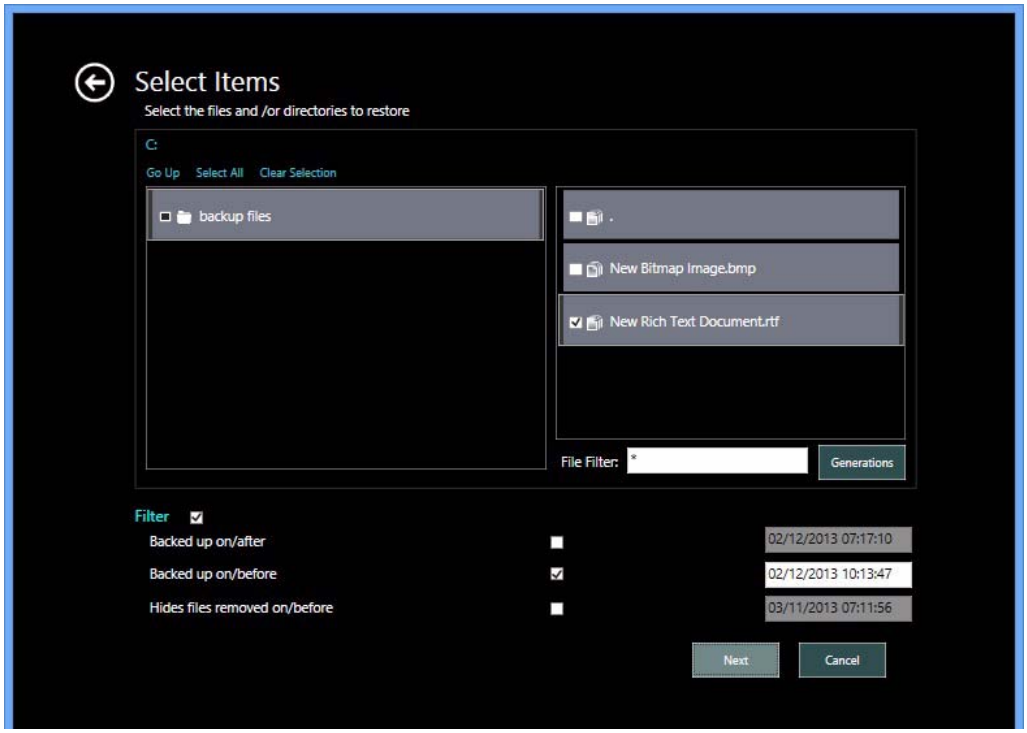
Restore

Restoring backup set data is always on-demand. You can select all or part of the backed up data, and apply various filters if you want only data from a particular time or fitting a particular pattern.

1. Highlight the backup set you want.
2. Click “Restore Now” or right-mouse click > Restore.



3. The Restore Data Wizard appears on the “Select Items” tab.

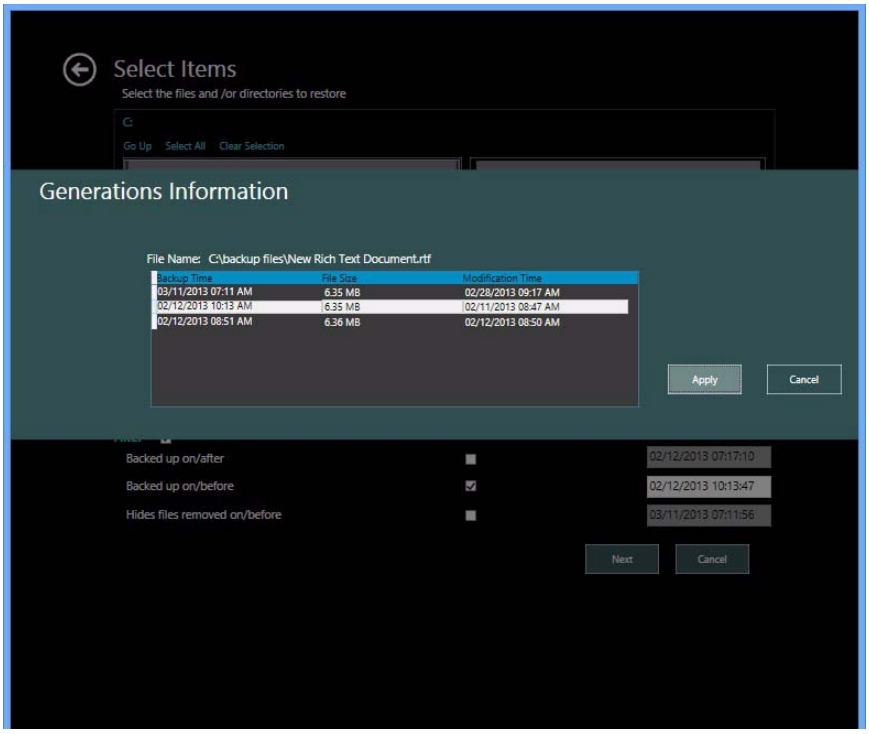


Dialog Help: See “Select Items (Restore)” on page 63.

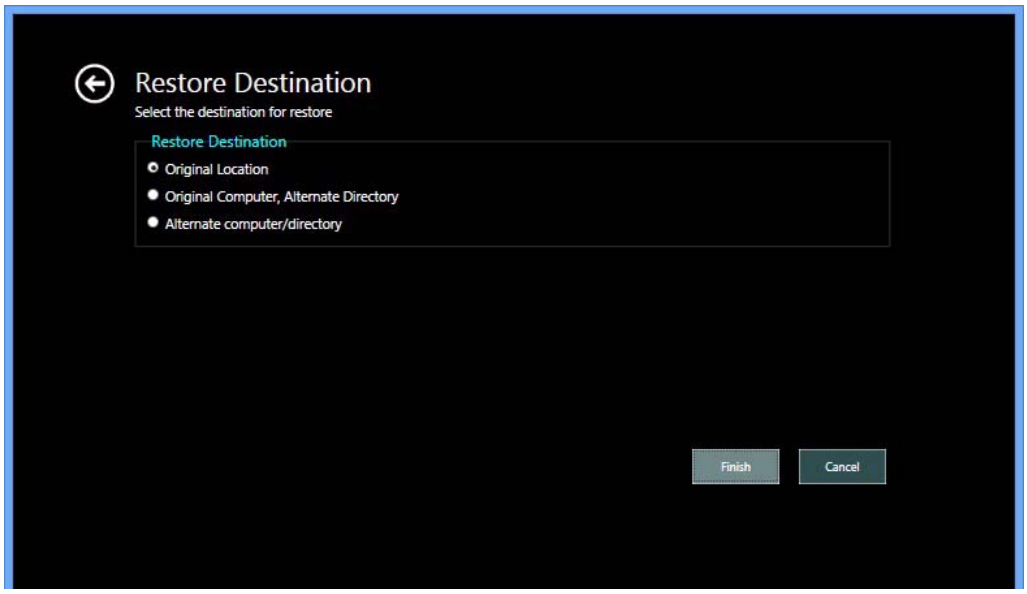
- Select the backed up items you want to restore.
- You can use the different filters to narrow the data you want to restore.

© Asigra Inc. All Rights Reserved.
Confidential.

- You can also select a specific generation to restore by highlighting a file and clicking “Generations”.



4. Once you have made your selection, click “Next”. The Restore Data Wizard appears on the “Restore Destination” tab.

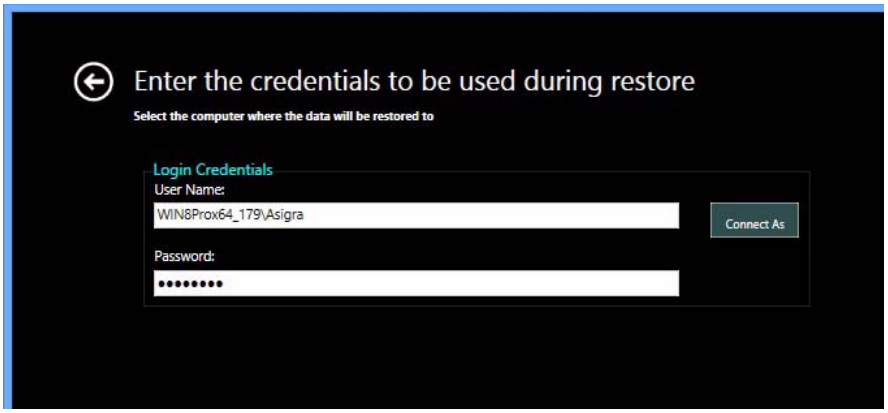


Dialog Help: See “Restore Destination” on page 61.

- **Original Location**: Click “Finish”.
- **Original Computer, alternate directory**: Click “Next”.

© Asigra Inc. All Rights Reserved.
Confidential.

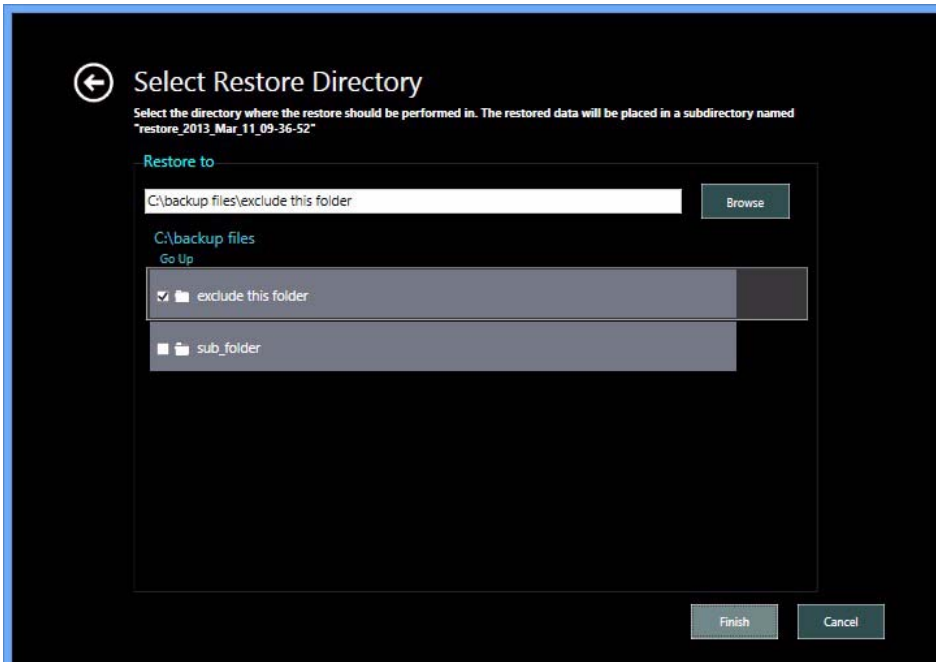
- The Restore Data Wizard appears on the “Use other credentials” tab. Supply the credentials for the restore folder and click “Next”.



Dialog Help: See “Use other credentials (Restore Data Wizard)” on page 65.

Dialog Help: See “Restore Destination Computer” on page 61.

- The Restore Data Wizard appears on the “Select Restore Directory” tab.

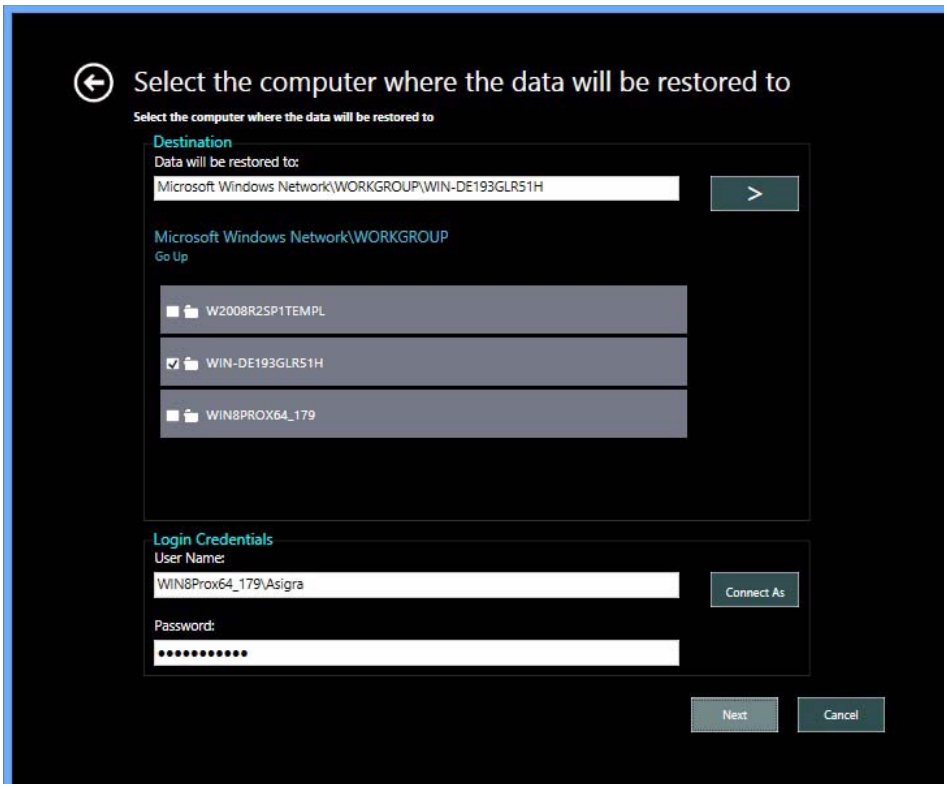


Dialog Help: See “Select Restore Directory” on page 64.

- Click “Browse” to select the restore folder.
- The Restore Data Wizard displays a “Browse Computer” section. Select the restore folder and click “Finish”.

© Asigra Inc. All Rights Reserved.
Confidential.

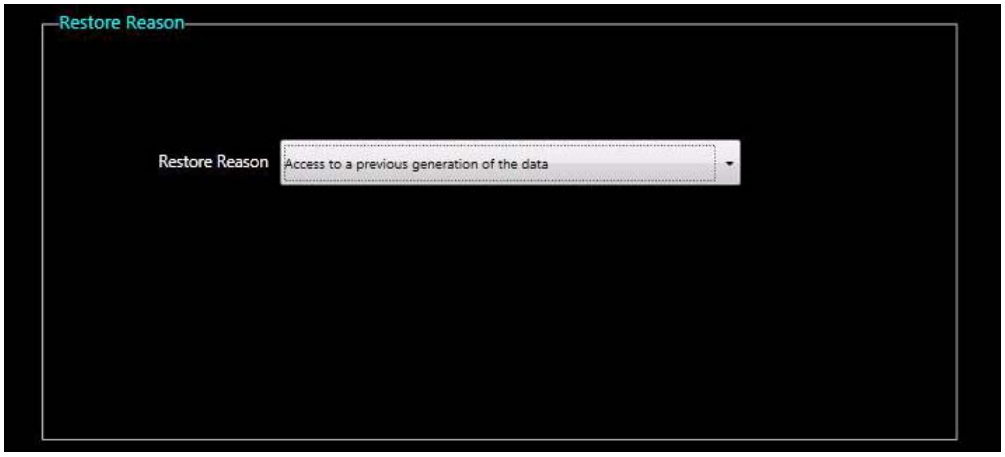
- **Alternate Computer / directory**: Click “Next”.
  - The Restore Data Wizard appears on the “Restore Destination Computer” tab.



Dialog Help: See “Restore Destination Computer” on page 61.

  - Select the destination computer and supply the credentials to that machine.
  - Click Next. The Restore Data Wizard appears on the “Select Restore Directory” tab. Select the restore folder and click “Finish”.

5. The Restore Data Wizard appears on the “Restore Reason” tab.



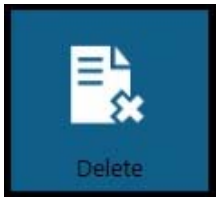
Dialog Help: See “Restore Reason” on page 61.

6. Select a reason from the drop-down list and click “Finish”. The restore will start immediately.
7. Check the Activity Log Tab for results. If you see any errors, you can check the Event Log.
   - See “Logs” on page 39.

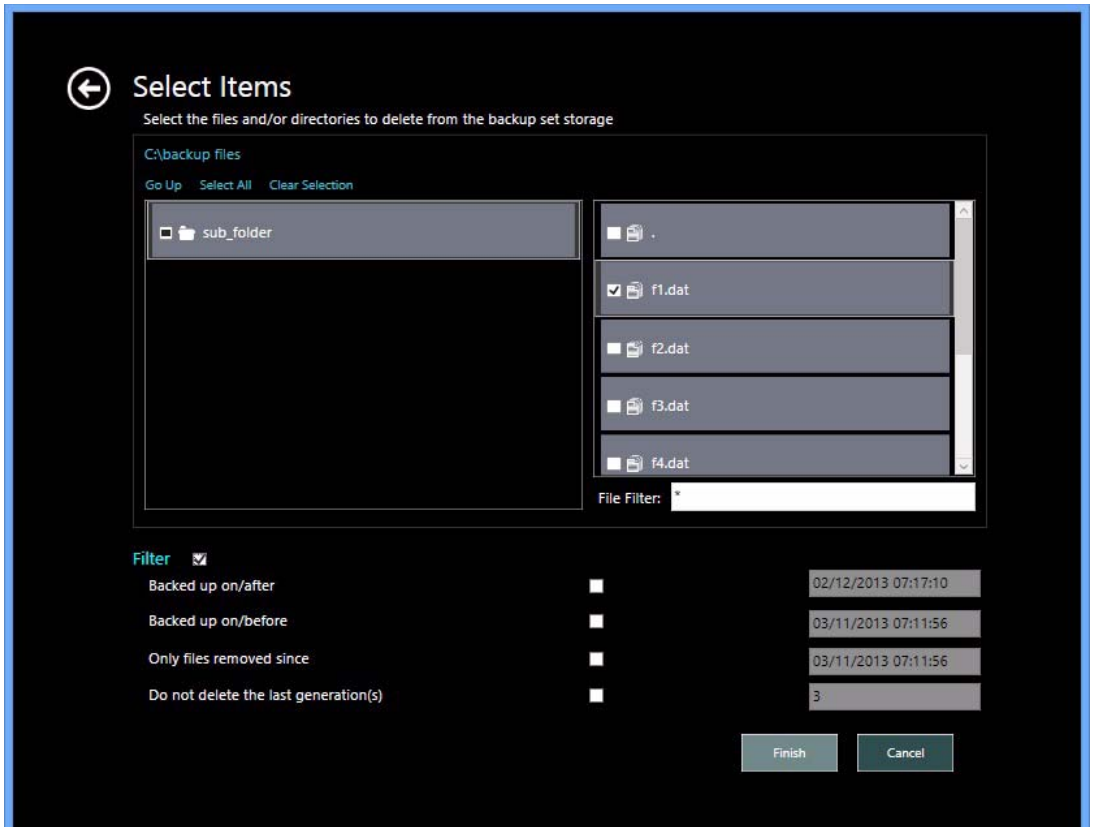
© Asigra Inc. All Rights Reserved.
Confidential.

Delete

1. Highlight the backup set you want.
2. Click “Delete” or right-mouse click > Delete.



2. The Delete Wizard appears on the “Select Items” tab.



Dialog Help: See “Select Items (Delete)” on page 62.

- Select the backed up items you want to delete.
- You can use the different filters to narrow the data you want to delete.

3. Click “Finish”. The delete will start immediately.
   - If you selected all the data, a popup will ask if you want to remove the set completely.
4. Check the Activity Log Tab for results. If you see any errors, you can check the Event Log.
   - See “Logs” on page 39.

© Asigra Inc. All Rights Reserved.
Confidential.

Synchronize

Synchronization compares the actual online storage on the DS-System with the DS-Mobile Client's database with to ensure it is correct.

1. Highlight the backup set you want.
2. Right-mouse click > Synchronize.

3. The synchronization will start immediately.
4. Check the Activity Log Tab for results. If you see any errors, you can check the Event Log.
   - See "Logs" on page 39.

Change Credentials

Changing credentials of a backup set may be necessary if required by your network security.

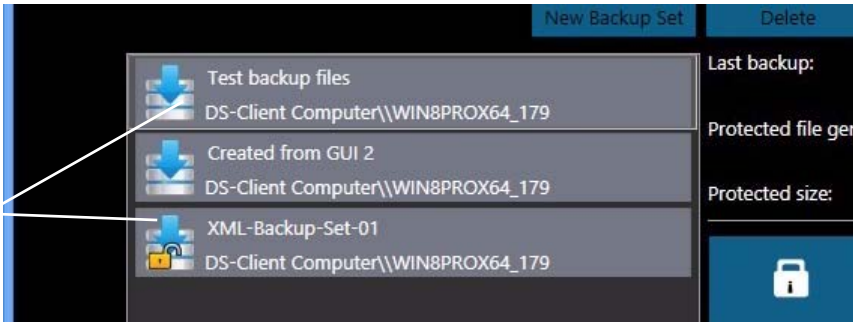
- See "Edit a Backup Set" on page 32.

© Asigra Inc. All Rights Reserved.
Confidential.

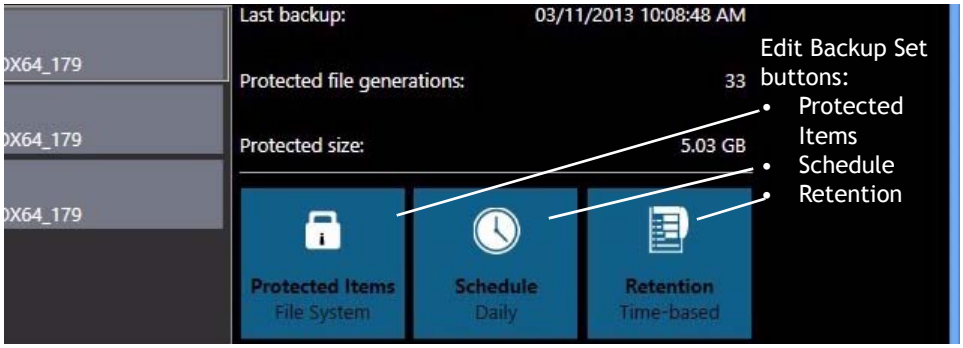
Edit a Backup Set

Backup sets are listed in the Asigra UI window. You can cycle through a long list with the TAB key.

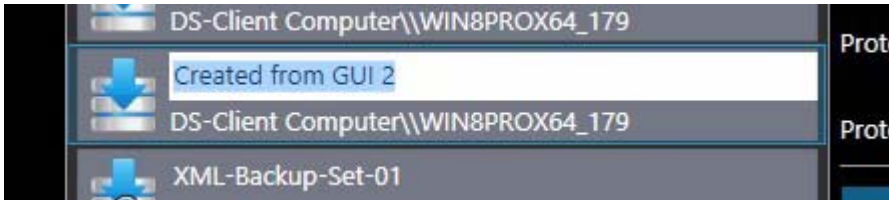
1. Highlight the backup set you want to edit from the list in the main Asigra UI window.



2. The backup set information section displays details about the set, and the properties buttons activate.



3. Click on one of the Edit Backup Set buttons to bring up the corresponding properties screen:
   - **Protected Items**: Opens a Protected Items Wizard. This Wizard's tabs are the same as when you created the backup set.
     - On the "Data Source and Login Information" tab, you can modify the credentials. (Dialog Help: See "Data Source and Login Information" on page 57.)
     - On the "Select Items" tab you can modify the backup items. (Dialog Help: See "Select Items (New / Edit Backup Set)" on page 62.)
   - **Schedule**: Opens a Schedule Wizard on the "Select Schedule" tab. This is the same tab as when you created the backup set. (Dialog Help: See "Select Schedule" on page 65.)
   - **Retention**: Opens a Retention Rule Wizard on the "Select Retention" tab. This is the same tab as when you created the backup set. (Dialog Help: See "Select Retention" on page 64.)
4. Edit the backup set's properties as required using these Wizards.
5. If you want to rename a backup set, double-click on its name in the list. Type in the new name and click outside the list to save your changes.



© Asigra Inc. All Rights Reserved.
Confidential.

Configuration & Logs

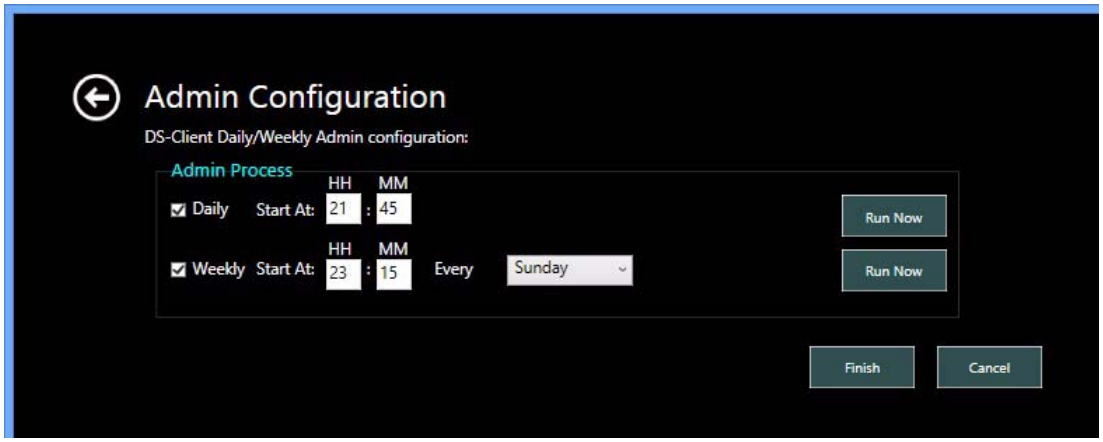
The following configuration options are available for DS-Mobile Client.

- See “Admin” on page 33.
- See “Re-Register” on page 34.
- See “Recovery” on page 35.
- See “DS-Mobile Client Configuration Tool” on page 36.
- See “Logs” on page 39.
- See “To update a DS-Mobile Client using ‘config-update.xml’” on page 40.
- See “About” on page 41.

Admin

1. Right-mouse click > Admin.

2. The Configuration Wizard appears on the “Admin Configuration” screen.



Dialog Help: See “Admin Configuration” on page 56.

- Select the Daily and Weekly Admin start times.

3. Click “Finish”.

© Asigra Inc. All Rights Reserved.
Confidential.

Re-Register

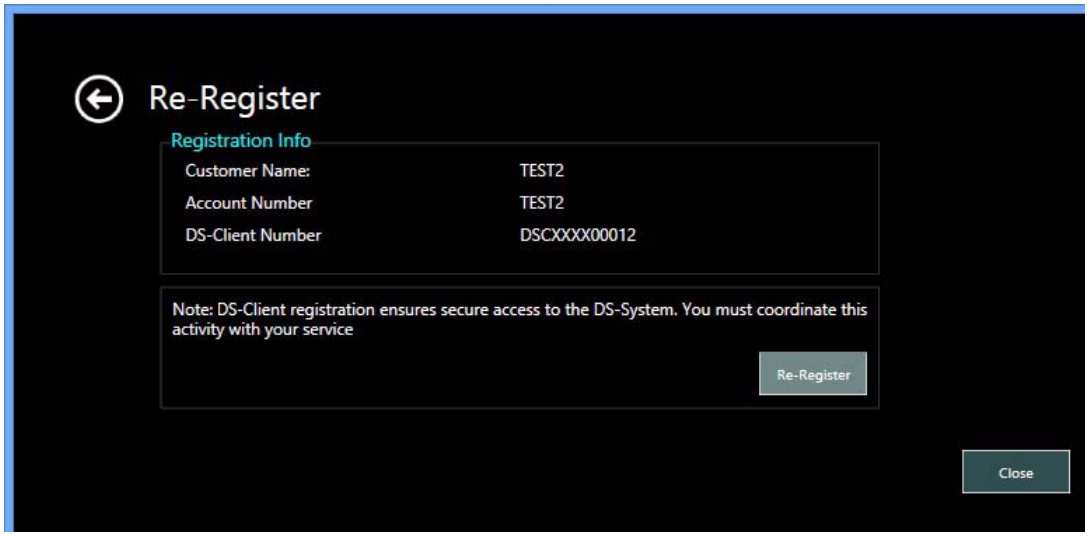
Your Service Provider may configure your DS-Mobile Client account to “Require Registration” with the DS-System in order to provide an extra level of security before backup data is accepted. If this is the case, the DS-Mobile Client is automatically registered with the DS-System during the first activity that requires connection.

THE ONLY SITUATION where you must re-register the DS-Mobile Client is if:

- The DS-Mobile Client computer’s hardware or operating system is replaced (or the DS-Mobile Client has been installed on a new machine).

To re-register your DS-Mobile Client with the DS-System:

1. Your Service Provider must permit re-registration with the DS-System. Arrange a time with your Service Provider when you will perform the Registration process. Your Service Provider will open a registration window (approximately 5 minutes) for you to complete the re-registration.
2. Right-mouse click > Re-Register.
3. The Re-Register screen appears.



Dialog Help: See “Re-Register” on page 60.

- Click “Re-Register”.

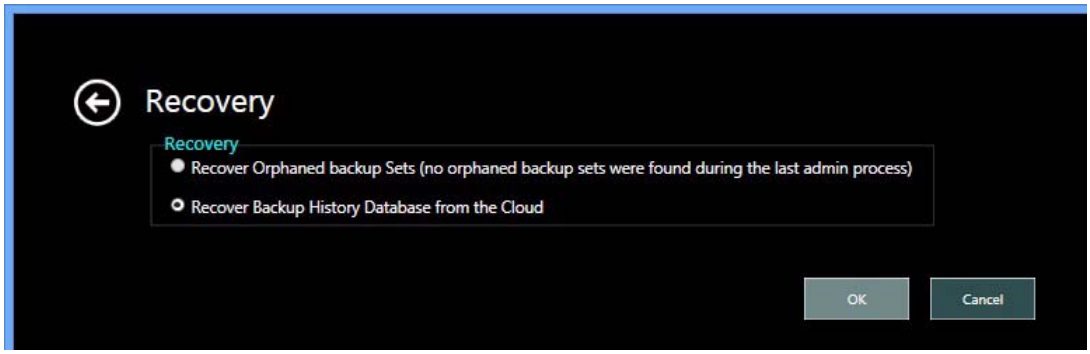
4. A message will appear informing you that registration was either successful, or that some error occurred and the reason why.

© Asigra Inc. All Rights Reserved.
Confidential.

Recovery

This option is only necessary if the DS-Mobile Client database has been damaged (or lost).

1. Right-mouse click > Recovery.
2. The Configuration Wizard appears on the “Admin Configuration” screen.


Recovery
Recovery
Recover Orphaned backup Sets (no orphaned backup sets were found during the last admin process)
Recover Backup History Database from the Cloud
OK
Cancel

Dialog Help: See “Recovery” on page 60.

- Select the DS-Mobile Client database recovery option.

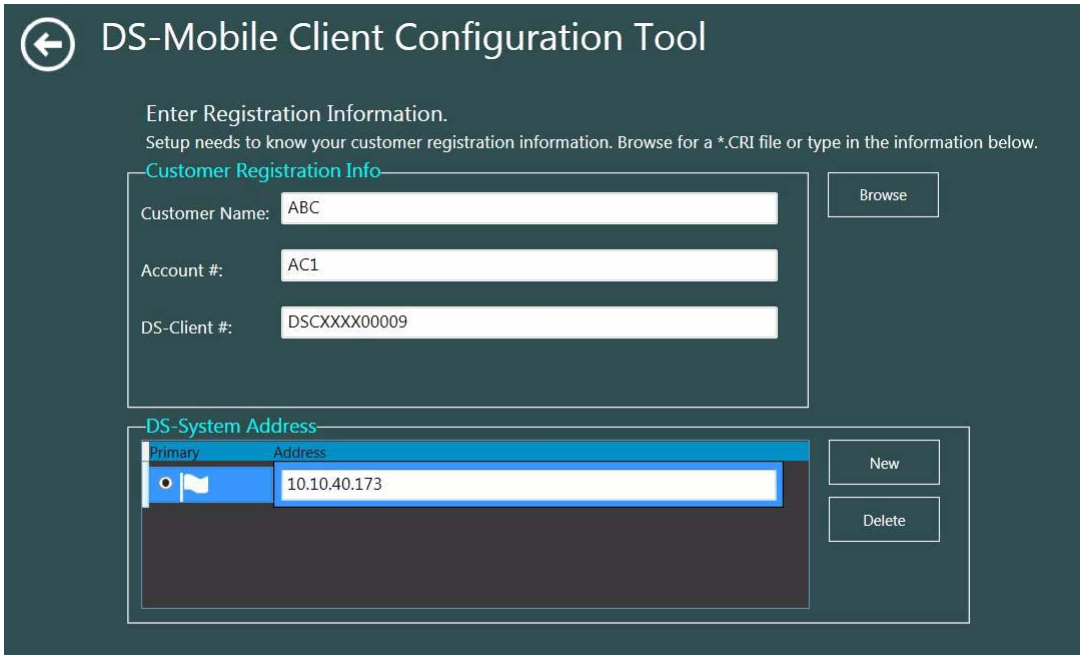
3. Click “OK”.

© Asigra Inc. All Rights Reserved.
Confidential.

DS-Mobile Client Configuration Tool

The DS-Mobile Client Configuration Tool is launched if you connect to a DS-Mobile Client that has not registered with a DS-System. You can also access it by right-clicking in the Asigra UI window and selecting “Settings”.

1. Right-mouse click > Settings.
2. The DS-Mobile Client Configuration Tool Wizard appears on the “Enter Registration Information” page.



Dialog Help: See “DS-Mobile Client Configuration Tool (Enter Registration Information)” on page 57.

3. In the “Customer Registration Info” section, enter the following:

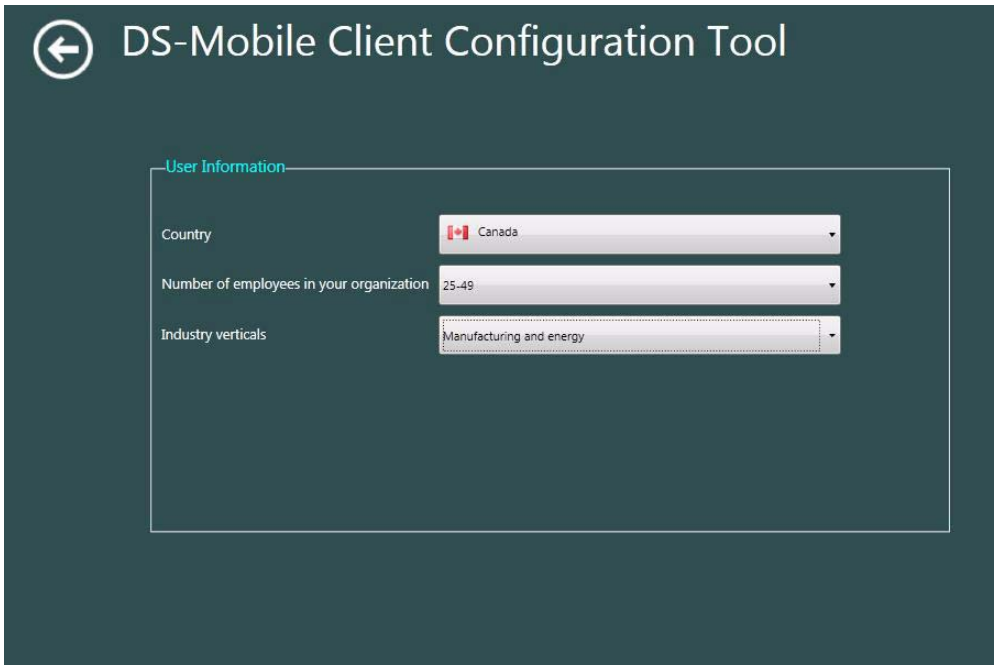
Customer Name	Enter a descriptive name for this DS-Mobile Client.
Account #	Enter your Account number. This number is provided to you by your Service Provider.
DS-Client #	Enter your DS-Client number. This number is provided to you by your Service Provider.

- **Browse**: An alternative to manually entering the above information is to use a .CRI file supplied by your Service Provider. Click “Browse” to search for this file on your network.

4. In the “DS-System Address” section, specify the DS-System connection information. You received the IP address of the DS-System from your Service Provider. The DS-Mobile Client requires this address in order for it to connect to the DS-System. In the “Address” field:
   - Enter the IP address of the DS-System your DS-Mobile Client will be using and click “Add”.
   - Your Service Provider may have more than one IP address for the DS-System, if this is the case you can specify any or all of them.

© Asigra Inc. All Rights Reserved.
Confidential.

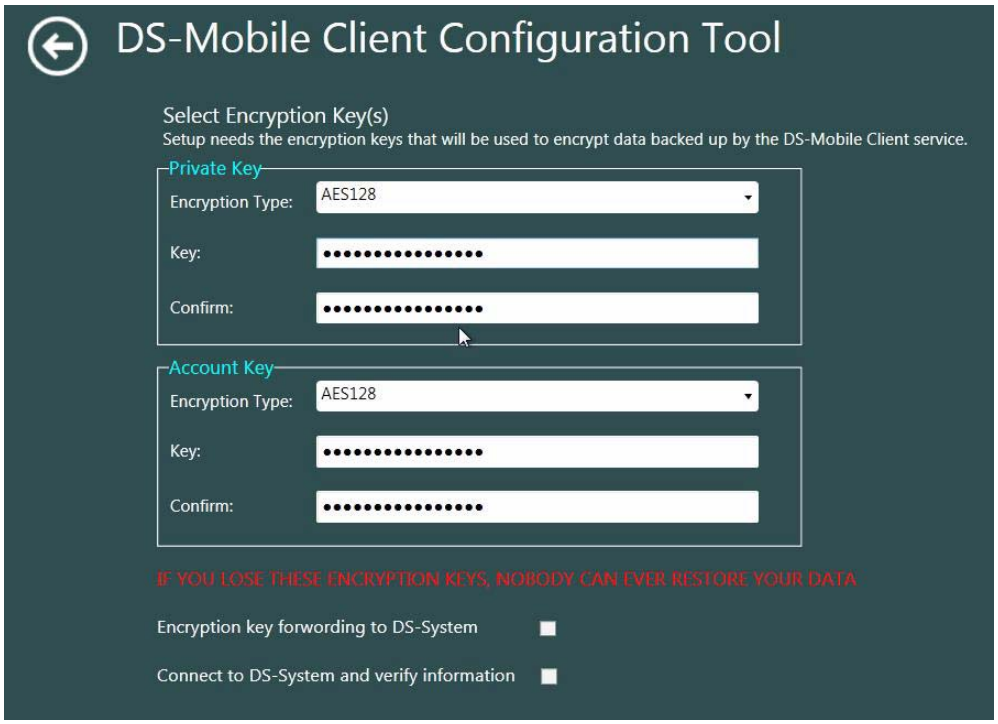
5. Click “Next”. The DS-Mobile Client Configuration Tool Wizard switches to the “User Information” tab.



Dialog Help: See “DS-Mobile Client Configuration Tool (User Information)” on page 58.

- You must supply the requested information about your organization by choosing from the drop-down list options.

6. Click “Next”. The DS-Mobile Client Configuration Tool Wizard switches to the “Select Encryption Key(s)” tab.



Dialog Help: See “DS-Mobile Client Configuration Tool (Select Encryption Keys)” on page 58.

© Asigra Inc. All Rights Reserved.
Confidential.

7. In the “Select Encryption Keys” section, you must set the encryption key(s) that the DS-Mobile Client will use.

Encryption Keys • An encryption key is case sensitive. Its length (in characters) depends on the type and level of encryption selected. DES requires 8 characters, AES-128 requires 16 characters, AES-192 requires 24 characters, and AES-256 requires 32 characters. For better security, do not use dictionary words or proper names, and try to randomly mix numbers in with the letters. • Auto-complete feature: If you do not specify the full amount of characters in the Key field, the GUI will fill in the remainder by repeating the string of characters you have entered. (e.g. entering “123” with AES-128 will generate an encryption key of “1231231231231231”, or entering “a” for DES will generate the encryption key “aaaaaaaa”). • Keep the key(s) in a secure location. Your ability to select the same encryption type and re-enter the same key is necessary if you ever need to reinstall your DS-Mobile Client to a new computer (e.g. if the computer is destroyed in a disaster).	
Private Key	You must set a private key for this DS-Mobile Client. Backup data from your DS-Client installation will be encrypted with this key. • **Type**: Select from the available types. Stronger encryption requires longer keys. • **Key**: Enter the key. • **Confirm**: Re-enter the key to verify the string is correct. You cannot change this key once it is set.
Account Key	You must set an account key if more than one DS-Mobile Client belongs to your customer account. Common backup data from all your DS-Client installations will be encrypted with this key. Once the account key is set, all DS-Clients from this customer must be configured with that same account key. • **Encryption Type**: Select from the available types. Stronger encryption requires longer keys. • **Key**: Enter the key. • **Confirm**: Re-enter the key to verify the string is correct. You cannot change this key once it is set.
Encryption key forwarding to DS-System • Check to have DS-Mobile Client forward the encryption key(s) to the DS-System the first time it connects with DS-System. NOTE: If you forward the keys, they will remain encrypted on the DS-System. However, your Service Provider will be able to create a valid .CRI file containing the encrypted keys. This file will be able to recreate a working version of this DS-Client. Make sure this conforms to your security policies before enabling this option.	
Connect to DS-System and verify information • Check to have DS-Mobile Client verify the configured information when you click “Finish”. A popup will appear explaining the results.	

8. Once you have made all the initial DS-Mobile Client configurations, click “Finish” to register with the DS-System.
   - If registration is successful, you will be able to use DS-Mobile Client immediately.

WARNING: If you change the Private Key after it has been set and this DS-Mobile Client is registered with the DS-System, this will cause DS-Mobile Client to fail to start.

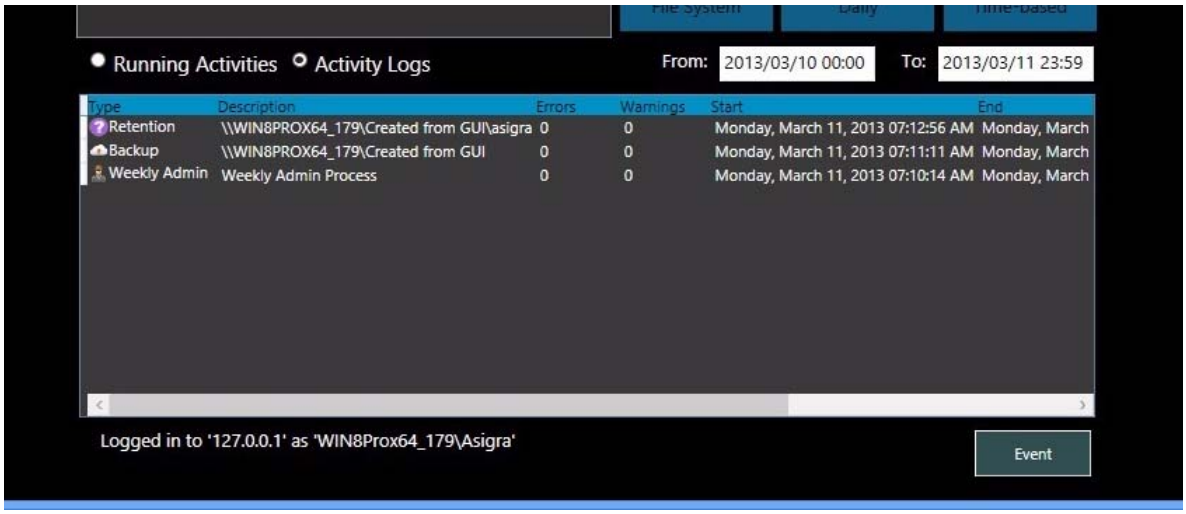
© Asigra Inc. All Rights Reserved. Confidential.

Logs

- See “Activity Log” on page 39.
- See “Event Log Viewer” on page 39.

Activity Log

The Activity Log Tab is visible from the main Asigra UI window.

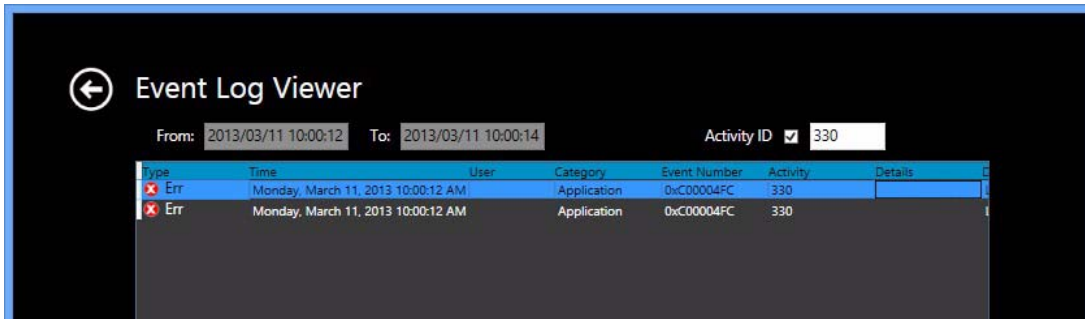


- You can expand or narrow the activities that are displayed using the “From” and “To” fields at the bottom.

Event Log Viewer

The Event Log provides more details about what occurred during DS-Mobile Client activities.

1. In the Activity Log Tab, highlight the activity whose events you wish to view.
2. Click the Events button. The Event Log Viewer appears.



Dialog Help: See “Event Log Viewer screen” on page 59.

© Asigra Inc. All Rights Reserved.
Confidential.

To update a DS-Mobile Client using 'config-update.xml'

On DS-Mobile Client, this functionality can create / update File System backup sets, user and group roles, backup schedules, and retention rules.

The XML file must be manually created by modifying the sample file (see: "SAMPLE 'config-update.xml' file" on page 42).

DS-Mobile Client will read any XML file named 'config-update.xml' and will verify that its structure is correct. If the file has not previously been applied, DS-Mobile Client applies any File System backup set configurations, schedules and retention rules.

Note: The XML file must be named "config-update.xml", and it must conform to the structure defined in the file "asigra_conf.dtd". Only the backup sets (File System type), roles, schedules, and retention rules from the XML file will be applied to the DS-Mobile Client database.

There are two update methods.

Method 1: Update locally from DS-Mobile Client

1. Create a 'config-update.xml' file for this DS-Mobile Client.
   - For an example, see "SAMPLE 'config-update.xml' file" on page 42.
   - For a list of variables you must change, see "Customizing the 'config-update.xml' file" on page 45.
2. Place the file 'config-update.xml' in the program folder containing the DS-Mobile Client service.
   - DS-Mobile Client checks for an updated 'config-update.xml' file every 10 seconds.
   - If updated, DS-Mobile Client will read the XML file and apply its settings.
   - After the XML file is applied, DS-Mobile Client renames the file to 'config-update-**nnn**.xml', where **nnn** is an incremental number.

Method 2: Update from DS-System (Service Provider)

The other method a 'config-update.xml' file can be distributed to a DS-Mobile Client is through the DS-System's Centrally Managed Backup Policy.

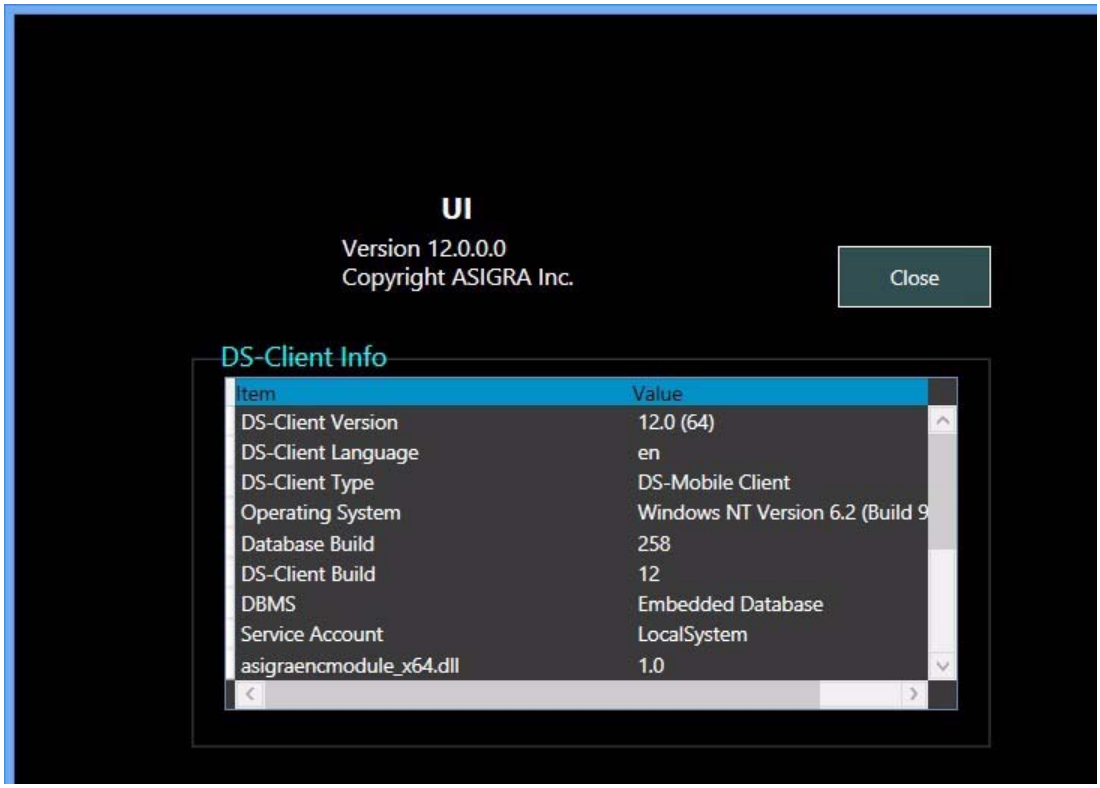
- See "Centrally Managed Backup Policy" on page 52.

© Asigra Inc. All Rights Reserved.
Confidential.

About

When logged in to DS-Mobile Client, you can view information about the current installation.

1. In the main Asigra UI window: Right-mouse click > About Asigra UI.
2. The “About DS-Client Info” screen appears.



Dialog Help: See “About” on page 56.

© Asigra Inc. All Rights Reserved.
Confidential.

SAMPLE ‘config-update.xml’ file

The following is a sample XML file.

- It will create one file system backup set named “XML-Backup-Set-01”, backing up “C:\Windows*.*” and all its sub-folders from the local (DS-Mobile Client) computer.
- The backup set uses the credentials of the user “Administrator” verified from the “domain_name” server. (A more realistic scenario would be “Administrator” from the local DS-Mobile Client computer itself.)
- The Regular Expression (RegEx) is an optional filter that, in this example only permits backup of files with the specified file extensions. Without this option, all items in the backup folder will be backed up.
- IMPORTANT NOTE: For each backup set you create, you must create a separate schedule and retention rule. Do not share a schedule or retention rule with different backup sets.

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE client-config SYSTEM "asigra_conf.dtd">
<client-config version="1.2">
    <schedules>
        <schedule name="Schedule-For-XML-Backup-Set-01" replace-existing="yes">
            <portable-schedule/>
            <schedule-details>
                <run-schedule>

                    <!-- GUI Monthly schedule option, cannot coexist with weekly schedule -->
                    <!-- <schedule-monthly every="1">
                        <schedule-on-month-day day="19"/>
                    </schedule-monthly> -->

                    <schedule-weekly every="1">
                        <week-day day="Mon"/>
                        <week-day day="Tue"/>
                        <week-day day="Wed"/>
                        <week-day day="Thu"/>
                        <week-day day="Fri"/>
                        <week-day day="Sat"/>
                        <week-day day="Sun"/>
                    </schedule-weekly>
                    <schedule-frequency>
                        <schedule-start when="14:00"/>
                        <schedule-end when="06:00" after-days="1"/>
                    </schedule-frequency>
```


© Asigra Inc. All Rights Reserved.
Confidential.

```
                <schedule-tasks run-retention="yes"/>
            </run-schedule>
        </schedule-details>
    </schedule>
</schedules>
<retentions>
    <retention-rule name="Retention-For-XML-Backup-Set-01" replace-existing="yes">
        <delete-options>
            <delete-removed unit="30" unit-type="days" generations="0"/>
        </delete-options>
        <retention-options>
            <retention-most-recent generations="1"/>
            <retention-time validity="1" validity-type="weeks">
                <retention-every unit="1" unit-type="days"/>
            </retention-time>
            <retention-time validity="1" validity-type="months">
                <retention-every unit="1" unit-type="weeks"/>
            </retention-time>

        <!--    <retention-time validity="1" validity-type="years">
                <retention-every unit="1" unit-type="months"/>
            </retention-time>  -->
        </retention-options>
    </retention-rule>
</retentions>
<backup-sets>
    <create-backup-sets>
        <new-file-system-backup-set>
            <basic-set-info name="XML-Backup-Set-01" owner="Administrator" owner-from="." replace-existing="yes"/>
            <source-server>
                <server-name>%ComputerName%</server-name>
                <net-provider>DS-Client Computer</net-provider>
            </source-server>
            <connect-as>
                <user-from use-client-account="no">.</user-from>
                <user-name>Administrator</user-name>
                <password ispwdhashed="yes">
                    aes-128-cbc$806867048F6EBBBF1CF97169811755F46A4FD8230D09BB59394840D37EA83D
                </password>
```


© Asigra Inc. All Rights Reserved.
Confidential.

```
                </connect-as>
                <file-system-items>
                    <file-system-item share-name="C:" path="\windows\*.*">
                        <file-system-item-backup-option option="permissions"/>
                        <file-system-item-backup-option option="alternate-streams"/>
                    </file-system-item>

                    <!-- Documents --> <regex-exclusion share-name="C:"
                    expression="\\.*\.(accdb|accde|accdr|accdt|csv|doc|docm|docx|dot|dotm|dotx|htm|html|mht|mpp|mppx|one|pdf|potm|po
                    tx|ppam|pps|ppsm|ppsx|ppt|pptm|pptx|ps|rtf|txt|vsd|wpd|wpg|wps|xlam|xlc|xls|xlsb|xlsm|xlsx|xlt|xltm|xltx)"
                    inclusion="yes"/>

                    <!-- Video --> <regex-exclusion share-name="C:"
                    expression="\\.*\.(asf|avi|dv|flv|m1v|m2p|m2v|m4v|moov|mov|mpa|mpe|mpeg|mpg|mpv|ogm|omf|qt|swf|vdo|vob|wm|wmd|wm
                    v|wmx)" inclusion="yes"/>

                    <!-- Picture --> <regex-exclusion share-name="C:"
                    expression="\\.*\.(ai|bmp|cdr|dib|eps|gif|icb|indd|j2c|j2k|jfif|jp2|jpc|jpe|jpeg|jpf|jpg|jpx|kdc|pcd|pct|pdd|pic
                    t|png|psd|psp|pxr|raw|rle|sct|tga|tif|tiff|vda|vst|wmf)" inclusion="yes"/>

                    <!-- Music --> <regex-exclusion share-name="C:"
                    expression="\\.*\.(a3c|aac|aif|aifc|aiff|ape|flac|itl|m3u|m4a|m4p|mid|midi|mp1|mp2|mp3|mp4|pls|ra|ram|rm|rmi|s3m
                    |wav|wma|wpl|xm)" inclusion="yes"/>

                    <!-- E-mails --> <regex-exclusion share-name="C:"
                    expression="\\.*\.(MsMessageStore|dbx|eml|fol|mbx|mif|msb|msf|msg|nsf|ost|pst|rwz|snm)" inclusion="yes"/>

                    <!-- Custom regex --> <regex-exclusion share-name="C:" expression="\\.*\.(CustomFileExtensions|doc|docx|mp3)"
                    inclusion="yes"/>

                </file-system-items>
                <generic-backup-options
                    schedule-name="Schedule-For-XML-Backup-Set-01"
                    retention-name="Retention-For-XML-Backup-Set-01"/>
            </new-file-system-backup-set>
        </create-backup-sets>
    </backup-sets>
</client-config>
```


© Asigra Inc. All Rights Reserved.

Confidential.

Customizing the 'config-update.xml' file

The previous sample config-update.xml file can be modified to create / update your own backup set. You must replace the following bold parameters in the file with your own values that reflect the backup set you want to create / update on the DS-Mobile Client (Changing any of the other parameters is optional.):

```
<basic-set-info name="YourBackupSetName" owner="UserName" owner-from="Where" replace-existing="yes"/>
```

```
<user-from use-client-account="no">Where</user-from>
```

Note: To indicate the local (DS-Mobile Client) computer, use the "." character (e.g. <user-from>.</user-from>).

Note 2: To use the DS-Mobile Client service's credentials, set the attribute use-client-account to "Yes" (e.g. <user-from use-client-account="yes">.</user-from>). This can only be done for backups of the local machine.

```
<user-name>UserName</user-name>
```

Note: This must be an existing user account that can be validated on the computer specified between the <user-from> tags.

```
<password ispwdhashed="yes">aes-128-cbc$58E9936316D9EC3659AEE014DC5CCD69D5455D9803A6BB40D50F5F8309599496</password>
```

Note: The encrypted user password code can be generated from the AsigraEncGUI.exe tool. This will produce a text file starting with "aes-128-cbc$...". Copy and paste that entire string between the <password> tags. A simpler, but much less secure method is to use "ispwdhashed="no" and type the plain-text password between the tags.

```
<file-system-item share-name="Drive Name" path="\YourDataPath\*.*" generations="3">
```

```
<regex-exclusion share-name="Drive Name" expression="Your own regular expression" inclusion="yes"/>
```

Note: The <regex-exclusion> element is optional. Do not include it if you want to backup all files in a directory. For simplicity, you can copy one of the sample regular expressions and replace the file extensions. If you set inclusion="no", then it inverts the regular expression (meaning it will backup any files that match the regular expression pattern).

```
<delete-removed unit="30" unit-type="days" generations="0"/>
```

Note: The <delete-removed> attribute is placed between the <delete-options> element tags. It configures the Retention process to remove backed up data that DS-Client detected was removed from the backup source machine. In the above sample, data removed from the backup source 30 days ago or longer would be deleted from online, leaving 0 generations online.

© Asigra Inc. All Rights Reserved.
Confidential.

SAMPLE 2: 'config-update.xml' file to assign DS-Mobile Client Roles

The following is a sample XML file.

- It will create / update four roles: a group role for users belonging to a Domain User Group, a user role for a specific Domain User, a group role for users belonging to a User Group on the local computer, and a user role for a specific local user.

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE client-config SYSTEM "asigra_conf.dtd">
<client-config version="1.2">
    <roles-config>
        <group-role role="administrator" name="Domain Users Group" from="Domain_Name"/>
        <user-role role="administrator" name="Domain_User_Name" from="Domain_Name"/>
        <group-role role="administrator" name="Local User Group" from="."/>
        <user-role role="administrator" name="Local_User_Name" from="."/>
    </roles-config>
</client-config>
```

SAMPLE 2: Customizing the 'config-update.xml' file to assign DS-Mobile Client Roles

The above sample config-update.xml file can be modified to add / update the 'administrator' role to a specific user account (either on the local DS-Mobile Client computer or from the Windows Domain). You must replace the following bold parameters in the file with your own values:

```
<group-role role="administrator" name="Domain Users Group" from="Domain_Name"/>
```

Note: This assigns the 'administrator' role to all members of the "Domain Users Group" domain user group. This must be an existing Domain User Group that can be validated against the Domain ("Domain_Name").

```
<user-role role="administrator" name="Domain_User_Name" from="Domain_Name"/>
```

Note: This assigns the 'administrator' role to the specific user "Domain_User_Name". This must be an existing Domain User that can be validated against the Domain ("Domain_Name").

```
<group-role role="administrator" name="Local User Group" from="."/>
```

Note: This assigns the 'administrator' role to all members of the "Local User Group" user group on the DS-Mobile Client computer. To indicate the local (DS-Mobile Client) computer, use the "." character for the "from" parameter.

```
<user-role role="administrator" name="Local_User_Name" from="."/>
```

Note: This assigns the 'administrator' role to the specific user "Local_User_Name" on the DS-Mobile Client computer. To indicate the local (DS-Mobile Client) computer, use the "." character for the "from" parameter.

© Asigra Inc. All Rights Reserved.
Confidential.

Knowledge Base

The Knowledge Base contains articles on specific areas of DS-Mobile Client operation.

© Asigra Inc. All Rights Reserved.
Confidential.

Backup & Restore of individual E-Mails from Microsoft Outlook

Creation Date: March 06, 2010
Revision Date: March 06, 2010
Product: DS-Mobile Client

Summary

DS-Mobile Client provides the “E-Mail” option when creating new backup sets. This will apply a filter to the selected backup folders that includes the various known file extensions belonging to major E-Mail applications (e.g. .ost or .PST for Microsoft Outlook).

This article provides an overview of different approaches you can take when you only want to back up individual E-Mails from Microsoft Outlook.

Backup

The steps described in this section include references to Microsoft Outlook. Some commands may be slightly different, depending on the version of Microsoft Outlook that you are backing up.

1. Use Asigra UI to create a backup set to backup E-Mails from a specific location you create for this purpose (e.g. “C:\MyOutlookBackupFolder”).
   - Open Asigra UI.
   - Click the “New Set” button from the Tool Bar.
   - Click Next.
   - In the “Select Items” page, check “E-Mail” (do not select any other file types) and specify the data location to be “C:\MyOutlookBackupFolder”.
   - Set up the schedule and retention (if required).
   - Give the backup set a name and click Finish.
2. Use Microsoft Outlook to select the E-Mails you want to backup. There are two different approaches you can take:

Select E-Mails by filtering through the Import and Export Wizard to an Outlook data file

In this approach, you export the E-Mail(s) you want to a file. You can apply a series of filters (time, subject, sender, etc.) to limit the information exported.

- Open Microsoft Outlook
- Choose File > Import and Export…
- Choose “Export to a file” and click Next.
- Choose “Personal Folder File (.PST)” and click Next.
- Select the Inbox.
  - Click Filter and specify which E-Mail(s) you want to backup.
- Click Next. Set the file location to C:\MyOutlookBackupFolder

  Tip: Give the file a meaningful name so you will know what is inside that file later on (e.g. C:\MyOutlookBackupFolder\backup_20100301.PST).
- Click “Finish”. You will be prompted to set properties for the .PST file.
  - In the Name field type a descriptive name like "Backup of E-Mails from March 1st”.
  - Click “OK” to start the export.

© Asigra Inc. All Rights Reserved. Confidential.

Create an Outlook data file and manually choose E-Mails by dragging and dropping

In this approach, you export the E-Mail(s) you want to a file by manually placing them in the target backup folder.

- Open Microsoft Outlook
- Choose File > Data File Management…
- In the “Data File” tab, click the “Add…” button, then click OK.
- Set the “Save in:” location to C:\MyOutlookBackupFolder
- Type in the file name what you like (e.g. backup_20100301.PST) and Click OK
- Give the personal folder a name (e.g. E-Mail Backup) and click OK.
- You will see an additional set of folders added to your folder list. Add a new folder ”Inbox” under “E-Mail Backup”
- Drag and drop the E-Mails you want to backup into Inbox of E-Mail Backup.
- Close “E-Mail Backup" when you are finished.

3. The selected E-Mails will be backed up on schedule. If you want to backup immediately, highlight this backup set and click the Backup button in Asigra UI.
4. Repeat the step 2 and 3 to selectively backup more E-Mails in future.
   - It is recommended that you use different .PST file names for different E-Mails.

Restore

Note: It is recommended that you close Microsoft Outlook before restoring.

1. Use Asigra UI to restore the .PST file on your computer.
   - Open Asigra UI.
   - Select the backup set and click the Restore button.
   - Select the .PST file you want to restore (e.g. backup_20100301.PST. You may have several .PST files, therefore descriptive names help).
   - Click Next and Finish the restore.
2. Use Microsoft Outlook to import the .PST file (Outlook data file). You can import the E-Mails using the following approaches:

Restore all E-Mails from an Outlook data file through the Import and Export Wizard

- Open Microsoft Outlook
- Choose File > Import and Export…
- Choose “Import from another program or file”.
- Choose “Personal Folder File (.PST)”.
- Select the .PST file you restored (e.g. C:\MyOutlookBackupFolder\ backup_20100301.PST)
- Set the options to "Include subfolders" and "Import items into the same folder in:" and select the folder that is listed in the dropdown list.
- Click Finish to complete the import.

Restore selective E-Mails by dragging and dropping them from an Outlook data file

- Open Microsoft Outlook
- Choose File > Open > Outlook Data File…
- Select the .PST file you restored (e.g. C:\MyOutlookBackupFolder\ backup_20100301.PST)

© Asigra Inc. All Rights Reserved. Confidential.

- You will now see an additional set of folders added to your folder list which you can expand. Expand the list and select the Inbox folder.
- In this folder select the messages you want to restore to the original Inbox folder
- Drag & drop them to the default Inbox folder.
- Close the additional set of folders that you just added from your folder list.

The information provided in this document is provided "AS IS", without warranty of any kind. ASIGRA Inc. (ASIGRA) disclaims all warranties, either express or implied. In no event shall ASIGRA or its business partners be liable for any damages whatsoever, including direct, indirect, incidental, consequential, loss of business profits or special damages, even if ASIGRA or its business partners have been advised of the possibility of such damages. © Asigra Inc. All Rights Reserved. Confidential.

© Asigra Inc. All Rights Reserved. Confidential.

Troubleshooting: Remote backup of Windows 7 / Windows 8 files requires a Microsoft patch and some configurations

Creation Date: June 30, 2010
Revision Date: September 26, 2012
Product: DS-Mobile Client

Summary

When DS-Mobile Client is installed on Windows Vista or Windows 2008 (all supported versions), you are not able to backup Windows 7 or Windows 8 files (Windows 2008 R2 files are not supported either, but DS-Mobile Client is not supposed to backup any server files).

The following configurations need to be done before you backup a Windows 7 / Windows 8 file:

1. Go to the services panel, enable 'Remote Registry' service.
2. Configure 'Remote Registry' service to automatically start.
3. Apply Microsoft fix: KB973278.

After these configurations, you should be able to backup remote Windows 7 / Windows 8 files.

The information provided in this document is provided "AS IS", without warranty of any kind. ASIGRA Inc. (ASIGRA) disclaims all warranties, either express or implied. In no event shall ASIGRA or its business partners be liable for any damages whatsoever, including direct, indirect, incidental, consequential, loss of business profits or special damages, even if ASIGRA or its business partners have been advised of the possibility of such damages. © Asigra Inc. All Rights Reserved. Confidential.

© Asigra Inc. All Rights Reserved. Confidential.

Centrally Managed Backup Policy

Creation Date: January 10, 2011
Revision Date: January 10, 2011
Product: DS-Mobile Client

Summary

This is enabled by your Service Provider from the DS-System side.

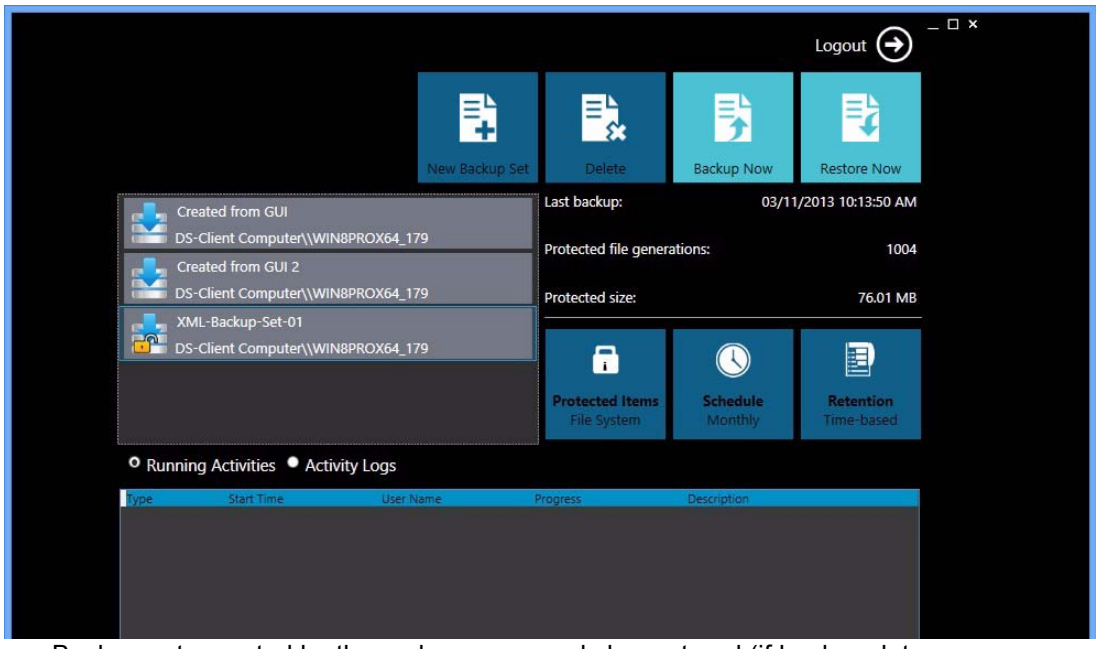
If a Centrally Managed Backup Policy is enabled for this DS-Mobile Client, it means all configurations (backup sets, schedules, retention rules, etc.) are managed by the DS-System. You will only be able to perform on-demand backups and selective restores from existing backup sets.

Details

If a Centrally Managed Backup Policy is enabled, some menus will be disabled and any backup sets created by the policy will have the image of a lock super-imposed over the backup set icon.

- DS-Mobile Client checks for a (new) policy on every connection with DS-System. This covers the configurations for backup sets, schedules, and retention rules.
- DS-Mobile Client skips any policies that have already been applied.
- Policies are configured from the DS-System side in an XML file. This file is downloaded to the DS-Mobile Client installation directory and applied as a standard 'config-update.xml' file. (For a description of how this is manually performed from the DS-Mobile Client side, see section "To update a DS-Mobile Client using 'config-update.xml'" on page 40).

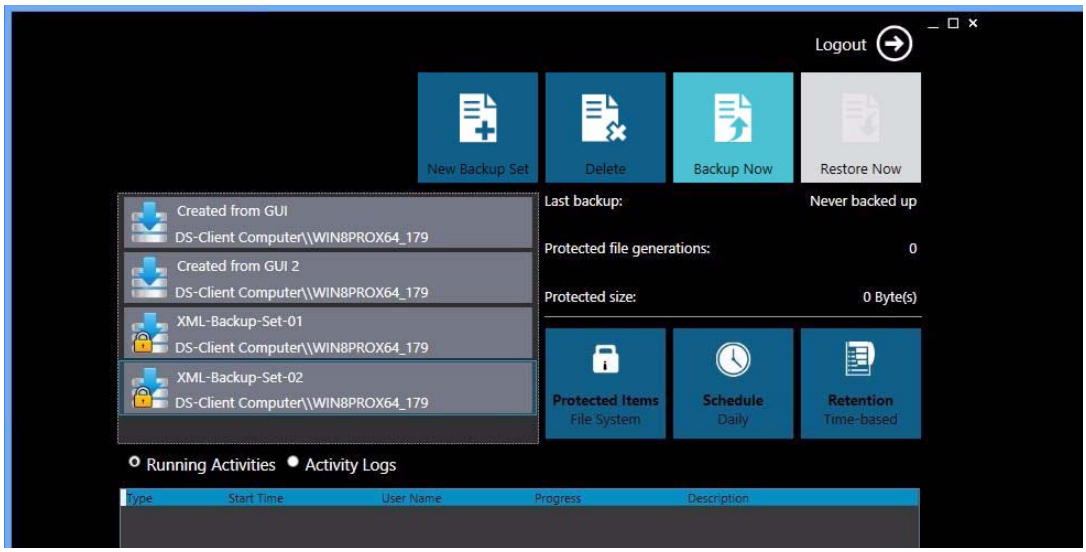
1. When a Centrally Managed backup policy is enabled, the backup set list in the Asigra UI window will identify the sets that are managed by the Service Provider (from the DS-System side) with a 'lock' icon.



- Backup sets created by the end-user may only be restored (if backup data exists online) or deleted. They cannot be backed up.

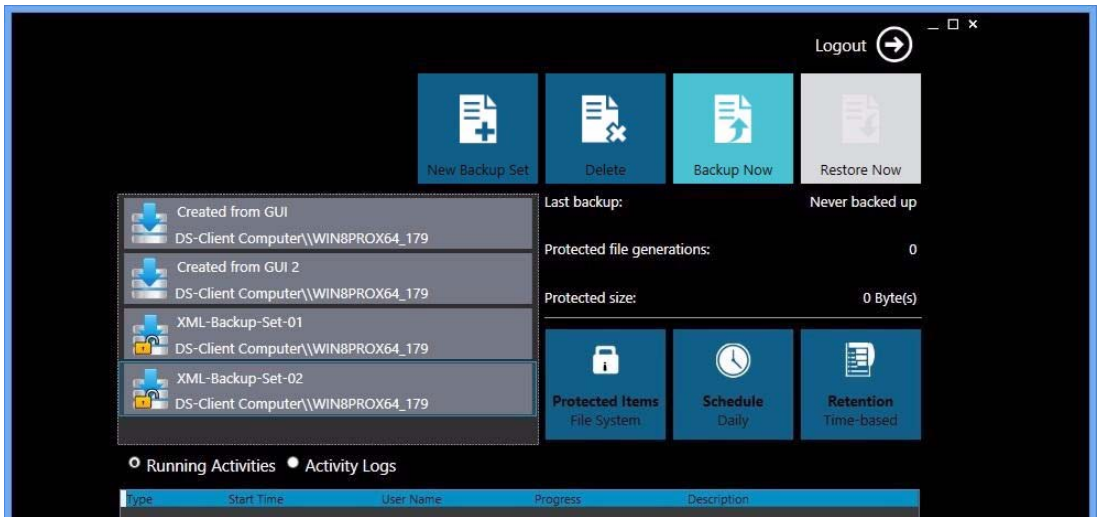
© Asigra Inc. All Rights Reserved.
Confidential.

2. Backup sets created by the Centrally Managed Backup Policy will appear with a ‘lock’ icon superimposed.



- From the Asigra UI window, you will only be able to perform on-demand backups and restores. All other tasks are scheduled according to the instructions from the DS-System.

3. If your Service Provider turns off the Centrally Managed Backup Policy, the control over the backup sets returns to the end-user through the Asigra UI window.



- Backup sets created by the Centrally Managed Backup Policy will appear with an ‘unlock’ icon superimposed.
- All backup sets will be configurable from the Asigra UI window (backup / restore / delete).

REMINDER:This feature is completely controlled from the DS-System (Service Provider) side.

The information provided in this document is provided "AS IS", without warranty of any kind. ASIGRA Inc. (ASIGRA) disclaims all warranties, either express or implied. In no event shall ASIGRA or its business partners be liable for any damages whatsoever, including direct, indirect, incidental, consequential, loss of business profits or special damages, even if ASIGRA or its business partners have been advised of the possibility of such damages. © Asigra Inc. All Rights Reserved. Confidential.

© Asigra Inc. All Rights Reserved. Confidential.

DS-NOC monitoring connections

Creation Date: August 31, 2011
Revision Date: August 31, 2011
Product: DS-Mobile Client

Summary

Note: The information in this article describes behavior that is transparent to DS-Mobile Client users. No configurations are required.

A DS-Mobile Client can be configured for monitoring by a DS-NOC (Network Operation Control) server. It must be enabled (either by you or your Service Provider) from the DS-NOC server. This means your DS-Mobile Client will send event information (backup logs) to the DS-NOC for monitoring purposes.

Connections to the DS-NOC are attempted in the following order:

1. Auto-detect Proxy Server
   - DS-Mobile Client automatically tries to detect if its network environment is using a proxy server. If it can detect and use the proxy server, then connection to DS-NOC will be performed through it. If it fails to detect a proxy server, DS-Mobile Client will attempt a direct connection to DS-NOC server.
2. Direct connection to DS-NOC server
   - DS-Client connects directly to DS-NOC. The protocol (HTTP or HTTPS) will be automatically selected based on the DS-NOC address.

The information provided in this document is provided "AS IS", without warranty of any kind. ASIGRA Inc. (ASIGRA) disclaims all warranties, either express or implied. In no event shall ASIGRA or its business partners be liable for any damages whatsoever, including direct, indirect, incidental, consequential, loss of business profits or special damages, even if ASIGRA or its business partners have been advised of the possibility of such damages. © Asigra Inc. All Rights Reserved. Confidential.

© Asigra Inc. All Rights Reserved. Confidential.

Dialog Help for Asigra UI screens

Dialog Help provides descriptions for the contents of the different GUI screens of the Asigra UI. It differs from the DS-Mobile Client Manual sections, which provide step-by-step instructions.

© Asigra Inc. All Rights Reserved.
Confidential.

Dialog Help

This section contains the Dialog Help for individual screens in the Asigra UI.

About

This screen shows information about the current Asigra UI and when logged in, the information about the DS-Mobile Client.

Admin Configuration

Use this screen to configure the DS-Mobile Client administrative process times. For DS-Mobile Client users, you should normally keep the default settings.

Daily	Enter the time when you want to begin the Daily Admin process. • Clear this checkbox to disable scheduled Daily Admin processes. • **Run Now**: Click to run the Daily Admin process immediately.
Weekly	Enter the time when you want to begin the Weekly Admin process. Select the day in the corresponding dropdown list. • Clear this checkbox to disable scheduled Weekly Admin processes. • **Run Now**: Click to run the Weekly Admin process immediately.

Backup Options

This is optional. This screen allows you to configure the Local Storage option for this backup set.

Local Storage Options • Note: This tool only appears if it is enabled for this DS-Client by your Service Provider.	
Keep a local copy of the latest generations in	Select to activate this option. • The latest generation of this backup set's data will also be stored in the selected local storage location. • Browse: Click to browse for the location. Do not select a location that is part of this backup set.

Browse Computer (Restore Data Wizard)

Use this screen to browse for a target restore folder. Double-click to open a folder. Click "Go Up" to return to the parent folder. The current folder is listed at the top of this screen.

© Asigra Inc. All Rights Reserved.
Confidential.

Data Source and Login Information

Use this screen to specify a backup set's source computer and the user account that will be used to access the backup data.

Data Source	Normally, for laptops, you would use the default "My Computer" selection. • You can browse to select another machine, if networked, however that computer must be accessible by this DS-Mobile Client service in order to backup.
Login Credentials	The default is the same username and password as the one currently used to log into the Asigra UI. • **Use DS-Client Account**: Allows you to use the DS-Client service's account credentials to connect to the local (DS-Client) computer. This option is only available when you select "My Computer" as the Data Source.

DS-Mobile Client Configuration Tool (Enter Registration Information)

This screen allows you to make the initial DS-Mobile Client configurations required to connect to a DS-System. It automatically appears after login to an unregistered DS-Mobile Client.

Customer Registration Info	
Customer Name	Enter a descriptive name for this DS-Client. • This name appears in brackets after the computer name in the Java DS-User GUI's list of available DS-Client computers (when sorted by Name).
Account #	Enter your Account number. This number is provided to you by your Service Provider.
DS-Client #	Enter your DS-Client number. This number is provided to you by your Service Provider.
Browse	An alternative to manually entering this information is to use a .CRI file supplied by your Service Provider. • Click Browse to search for this file on your network.
DS-System Address	
Address	Enter an IP address or DNS name for the DS-System your DS-Mobile Client will be using. • A DS-System with multiple addresses can be entered on one line, with each address separated by a semi-colon (;). • If there is more than one connection configuration to the DS-System is supplied, you must indicate which one is "Primary" (i.e. the default that DS-Mobile Client will use).
New	Click to add a new connection to list.
Delete	Click to remove the highlighted connection from the list.

© Asigra Inc. All Rights Reserved.
Confidential.

DS-Mobile Client Configuration Tool (Select Encryption Keys)

This screen allows you to make the initial DS-Mobile Client configurations required to connect to a DS-System. It automatically appears after login to an unregistered DS-Mobile Client.

Encryption Keys • An encryption key is case sensitive. Its length (in characters) depends on the type and level of encryption selected. DES requires 8 characters, AES-128 requires 16 characters, AES-192 requires 24 characters, and AES-256 requires 32 characters. For better security, do not use dictionary words or proper names, and try to randomly mix numbers in with the letters. • Auto-complete feature: If you do not specify the full amount of characters in the Key field, the GUI will fill in the remainder by repeating the string of characters you have entered. (e.g. entering "123" with AES-128 will generate an encryption key of "1231231231231231", or entering "a" for DES will generate the encryption key "aaaaaaaa"). • Keep the key(s) in a secure location. Your ability to select the same encryption type and re-enter the same key is necessary if you ever need to reinstall your DS-Mobile Client to a new computer (e.g. if the computer is destroyed in a disaster).	
Private Key	You must set a private key for this DS-Mobile Client. Backup data from your DS-Mobile Client installation will be encrypted with this key. • **Encryption Type**: Select from the available types. Stronger encryption requires longer keys. • **Key**: Enter the key. • **Confirm**: Re-enter the key to verify the string is correct. You cannot change this key once it is set.
Account Key	You must set an account key if more than one DS-Mobile Client belongs to your customer account. Common backup data from all your DS-Client installations will be encrypted with this key. Once the account key is set, all DS-Clients from this customer must be configured with that same account key. • **Encryption Type**: Select from the available types. Stronger encryption requires longer keys. • **Key**: Enter the key. • **Confirm**: Re-enter the key to verify the string is correct. You cannot change this key once it is set.
Encryption key forwarding to DS-System • Check to have DS-Mobile Client forward the encryption key(s) to the DS-System the first time it connects with DS-System. NOTE: If you forward the keys, they will remain encrypted on the DS-System. However, your Service Provider will be able to create a valid .CRI file containing the encrypted keys. This file will be able to recreate a working version of this DS-Client. Make sure this conforms to your security policies before enabling this option.	
Connect to DS-System and verify information • If selected, when you click "Finish" DS-Mobile Client will connect to DS-System to verify the registration.	

DS-Mobile Client Configuration Tool (User Information)

This screen requires you to input information about your organization. It automatically appears after login to an unregistered DS-Mobile Client.

User Information • Country: Select your location. • Number of employees in your organization: Select from the drop-down list. • Industry vertical: Select from the drop-down list.

© Asigra Inc. All Rights Reserved. Confidential.

Main Window

Once you have successfully connected to the DS-Mobile Client, the Asigra UI Window activates.

Title Bar	Shows the login name and location (usually 127.0.0.1 for the local computer / laptop).
Backup Set List	Shows a list of the backup sets that have been defined on the DS-Mobile Client. If you click on a backup set, its properties are displayed to the right. The Action and Edit buttons will activate or be grayed out, depending on what can be performed. • You can highlight a backup set with the mouse or use the arrow keys to cycle through each set in the list. • To rename a backup set, double-click on its name.
Action Buttons	The action buttons (except New Backup Set) work on the backup set highlighted in the Backup Set List. • New Backup Set • Delete • Backup Now • Restore Now
Edit Buttons	The Edit buttons work on the backup set highlighted in the Backup Set List. • Protected Items • Schedule • Retention
Running Activities Tab	Shows any activities that are currently running on the DS-Mobile Client. If possible, you can use the Stop button to end the highlighted activity. • **Stop**: Click this button to try to stop a highlighted activity from the current activities list.
Activity Log Tab	Shows a list of all the activities logged by the DS-Mobile Client. You can filter the list by date. • **Events**: Click this button to open the Event Log Viewer for the highlighted activity.

Event Log Viewer screen

Use this screen to examine the Event Logs. This displays the error, warning, and information messages that occurred during DS-Mobile Client activities for the period selected.

Filter	
From	Type the earliest date you want to display in this field. No events older than this time forward will be displayed.
To	Type the latest date you want to display in this field. No events newer than this date and time will be displayed.
Activity ID	Enter a specific ID, to see only those events associated with that ID.
Event List	
Type	Shows the severity of the event that occurred: • Information message. • Warning message. • Error message.
Time	Shows the date and time that the event occurred.
User	Shows the name of the user associated with the event (if any).
Category	Shows the category of the message. The category can be any of the categories listed in the event Category drop down list.
Event Number	Contains an event ID code.
Activity	Contains the Session ID number associated with the event.
Detail	This field may display the IP connection (if applicable).

© Asigra Inc. All Rights Reserved. Confidential.

Description	Displays a description of the highlighted event.

Generations Information

Use this screen to select a specific generation of a file for restore. Highlight the generation you want in the list and click “Select”. The Restore Data Wizard will refresh to reflect the new backup selection.

Login

Use this screen to connect to the DS-Mobile Client service.

User Name	Type your User Name. This must be a valid, active account (Administrator-level) on the computer where the DS-Mobile Client service is running.
Password	Type your password.
From	Select the domain or server on which the username and password will be verified. (i.e. DS-Mobile Client validates supplied credentials with this domain or server.) • This option only appears if the DS-Mobile Client computer belongs to a Windows Domain.
Use currently logged in user	Select this option to use your current logged on Windows Username and Password to connect to the DS-Mobile Client.

Re-Register

Use this screen to re-register the DS-Mobile Client’s hardware information with the DS-System.

Registration Info section	
Customer name	Your customer account name.
Account #	Your customer account number on DS-System.
DS-Client #	This DS-Mobile Client's number on DS-System.
Re-Register section	
Re-Register	Click to re-register this DS-Mobile Client’s hardware installation with the DS-System. • This must be performed together with your Service Provider, who must permit the DS-Mobile Client to re-register. • For details, see: “Re-Register” in the User Guide.

Recovery

Use this screen to specify recovery of information for the DS-Mobile Client itself.

Recover Orphaned Backup Sets	Orphaned sets are found by the DS-Mobile Client’s Daily Admin. / Weekly Admin. process. If this option can be selected, it means ‘orphaned’ backup sets were discovered on the DS-System: backup set data exists on the DS-System, but the corresponding backup settings do not exist in the DS-Mobile Client database. (This is only likely to occur if that database is somehow lost or damaged.) • Select this option and click OK to recover each orphaned backup set’s configurations to the DS-Mobile Client’s database.

© Asigra Inc. All Rights Reserved. Confidential.

Recover Backup History Database from the Cloud	If the DS-Mobile Client's database is damaged, you can recover the last backed up version of this database from the DS-System using this option. • By default, the DS-Mobile Client's database is backed up as part of the Daily Admin process. • You will lose any changes made since the backup time of the database.

Restore Data Select Folder

This screen allows you to select the destination restore folder.

Restore Destination

Use this screen to select where you want to restore the data.

Original Location	Restores data to the same location from which it was backed up. • Overwrites any data of the same name. • If selected, you can click "Finish" to proceed with the restore.
Original Computer, Alternate Directory	Restores data to a different directory on the same source computer. • If selected, you can click "Next" to open a wizard to provide credentials and select the restore destination.
Alternate Computer / Directory	Restores data to a different computer. • If selected, you can click "Next" to open a wizard to provide credentials and select the restore destination.

Restore Destination Computer

Use this screen to select an alternate computer where you want to restore the data.

Destination	Click the [>] button to browse for the computer. • A "Select Computer" screen appears, allowing you to browse the networked computers for a destination.
Login Credentials	You must supply valid login credentials to any alternate destination computer you select. • Click the "Connect As" button to display the password field.
Next	Once finished making your computer selection, you can click "Next" to open the "Select Restore Directory" screen.

Restore Reason

This is mandatory. You must supply a reason for this restore by selecting from the drop down list.

Select Backup Set Name

Use this screen to specify a backup set's name. If you need to change the backup set name afterwards, you can double-click on it in the main Asigra UI window.

© Asigra Inc. All Rights Reserved. Confidential.

Select Computer

This screen allows you to select the source computer for backup or the destination computer for restore.

Select Folder (Add / Edit Backup Items)

This screen allows you to browse the backup source machine and select the backup items.

Select Items (Delete)

Use this screen to select a backup set's items for delete.

Select the files and/or directories to delete from the backup set storage The left side contains a folder list and the right side contains the files in the highlighted folder. Double-click to browse into the backed up folders from this backup set. When you highlight (single-click) a folder, the backed up files inside that folder are listed to the right. Double-click on the folder to browse one level deeper. • **Go up**: Navigate back to the top level folder. • **Select All** / **Clear Selection**: Applies to all backed up folders and files. • **File Filter**: This is a file name pattern filter (e.g. *.pdf means only files with the .pdf extension). The default is * (meaning "all files" in the highlighted folder will be displayed.	
Filter • Select to activate the filter section. Any filters selected will apply to what is displayed in the delete tree.	
Backed up on / after	Limits the Items to Delete display to directories / files backed up from this time.
Backup up on / before	Limits the Items to Delete display to directories / files backed up prior this time.
Only files removed since	This filter allows you to show only backed up data (directories and files) that was intentionally deleted from the source computer. • Select a date and time in this field to search for backed up data that was not scanned by the DS-Mobile Client since the filter date.
Do not delete the last generation(s)	Allows you to specify the number of generations to leave (i.e. not select for delete) from the specified period. • If you specify a number, you will only be able to select files and directories that have more generations online than the number specified in this field.

Select Items (New / Edit Backup Set)

Use this screen to specify a backup set's items.

Files To Backup	
All Files	If selected, all data at the selected backup location will be backed up. This is the equivalent of applying a *.* filter.

© Asigra Inc. All Rights Reserved.
Confidential.

Exclude Filters	If you selected “All Files”, you can also exclude files with known extensions that are never required for backup. Hover the cursor over the filter name to see what file extensions it will include: • Exclude temporary files • Exclude backup files • Exclude file extensions: This option allows you to specify the extension(s) to exclude. Multiple extensions can be separated by the “|” character. Extensions can be any length, as long as the file system accepts those characters.
Include Filters	If you do not select “All Files”, you must specify at least one of the inclusion filters. Hover the cursor over the filter name to see what file extensions it will include: • Documents • Videos • Music • Pictures • E-Mails • Custom file extensions: This option allows you to specify the extension(s) to include. Multiple extensions can be separated by the “|” character. Extensions can be any length, as long as the file system accepts those characters.
Data Location • Remember that backups of data at the Data Location will have the selected include / exclude filters applied.	
Specific Location	These are commonly backed up locations you might select for backup. • All User Documents: Backs up the “Documents” folder from the DS-Mobile Client computer’s \Documents and Settings\All Users path. • [...] Desktop: If logged in as user “Administrator”, this will show “Administrator’s Desktop”, allowing you to backup all items on this user account’s Windows desktop.
Custom	This section allows you to browse the accessible folders on the data source. • Add Backup Items: Opens a popup wizard browser for the target data location. You can add specific folders individually. Exclusions can be made for sub-folders of an added folder.

Select Items (Restore)

Use this screen to select a backup set’s items for restore.

Select files and / or directories to restore The left side contains a folder list and the right side contains the files in the highlighted folder. Double-click to browse into the backed up folders from this backup set. When you highlight (single-click) a folder, the backed up files inside that folder are listed to the right. Double-click on the folder to browse one level deeper. • **Go up**: Navigate back to the top level folder. • **Select All** / **Clear Selection**: Applies to all backed up folders and files. • **File Filter**: This is a file name pattern filter (e.g. *.pdf means only files with the .pdf extension). The default is * (meaning “all files” in the highlighted folder will be displayed. • **Generations**: Opens the “Generations Information” screen for the highlighted file in the file list.	
Filter	
Backed up on / after	Limits the Items to Restore display to directories / files backed up from this time.
Backup up on / before	Limits the Items to Restore display to directories / files backed up prior this time.

© Asigra Inc. All Rights Reserved. Confidential.

Hide files removed on / before	This filter allows you to hide backed up data (directories and files) that was intentionally deleted from the source computer. • Select a date and time in this field to screen out backed up data that was not scanned by the DS-Mobile Client since the filter date. • This prevents you from restoring directories / files that were intentionally deleted.

Select Restore Directory

Use this screen to select an alternate directory where you want to restore the data.

Restore To	Click "Browse" to select a restore directory. • To avoid any accidental overwrites, the data is always restored in a unique sub-directory named with the time when this restore request was started.
Finish	Click to proceed with the restore.

Select Retention

- Note: On DS-Mobile Client, time-based retention automatically runs after every backup process.

Use this screen to specify a backup set's retention policy. Retention is "what data you want to keep"; all other data will be removed from online storage. Note the implications of enforcing a retention policy: it limits data growth to the specified amount of generations, but it automatically deletes any data that does not meet the retention policy.

Time-based Online Retention	
Keep most recent generations	This is the maximum generations per file. • This is a mandatory default selection. It cannot be turned off. • Valid values from 1-9999, default is 3
Keep one generation per day for 1 week	This is optional. • Every time retention is enforced, at least one generation from each day of the past week will be kept.
Keep one generation per week for 1 month	This is optional. • Every time retention is enforced, one generation will be kept for the most recent month.
Keep one generation per month for 1 year	This is optional. • Every time retention is enforced, one generation will be kept for each month from the last year.
Retention for files deleted from source	
Apply retention if files have been removed from source	Select to activate this retention option. If selected, you must specify the following: • **Minimum age of deleted files**: This amount of time must have passed since the backed up file was removed from the source backup location. • **Number of generations to keep**: By default, this is set to '0' which means all generations will be deleted. If specified, this number of generations of the file will be kept online (the latest generations are kept).

© Asigra Inc. All Rights Reserved. Confidential.

Select Schedule

Use this screen to specify the schedule for a backup set.

Scheduling Type	
• No Schedule: If selected, the other sections will not appear. Only on-demand backups can be performed. • Daily Backups • Monthly Backups	
Scheduling Day(s)	
• Daily Backup: Checkboxes allow you to select each day of the week you want. • Monthly Backup: A field allows you to select a fixed day of the month (from 1-28).	
Start / End Time	
Start At	You must specify a start time. • **Retry backup if connection to cloud unavailable**: If selected, the DS-Mobile Client will retry the scheduled backup if it cannot connect to the DS-System at the scheduled time. Retries are attempted every minute.
Stop At	If selected, you must specify a fixed end time for the scheduled backup. If the backup has not finished by this time, the process will be stopped. • The drop down list allows you to select a schedule window of up to 6 days.

Use other credentials (Restore Data Wizard)

In this screen, you must enter the username and password to connect to the restore destination. Click “Connect As” to display the password field.

© Asigra Inc. All Rights Reserved.
Confidential.